

# A Torelli theorem for curves over finite fields

Fedor Bogomolov, Mikhail Korotiaev and Yuri Tschinkel  
*Courant Institute of Mathematical Sciences, N.Y.U.*  
*251 Mercer str., New York, NY 10012, U.S.A.*

*To John Tate, with admiration*

**Abstract.** We study hyperbolic curves and their Jacobians over finite fields in the context of anabelian geometry.

## 1. Introduction

This paper is inspired by the foundational results and ideas of John Tate in the theory of abelian varieties over finite fields. To this day, the depth of this theory has not been fully explored. Here we apply Tate's theorems to anabelian geometry of curves over finite fields.

Let  $C$  be an irreducible smooth projective curve of genus  $g = g(C) \geq 2$  defined over a field  $k$  and let  $C(k)$  be its set of  $k$ -rational points. When  $k$  is the field of complex numbers, the complex torus

$$H^0(C(\mathbb{C}), \Omega_C^1)^\vee / H_1(C(\mathbb{C}), \mathbb{Z})$$

is the set of complex points of an algebraic variety, the Jacobian variety  $J$  of  $C$ . Choosing a point  $c_0 \in C(\mathbb{C})$  we get a map

$$\begin{aligned} C(\mathbb{C}) &\rightarrow J(\mathbb{C}) \\ c &\mapsto (\omega \mapsto \int_\gamma \omega), \end{aligned}$$

where  $\omega \in \Omega_C^1$  is a global section of the sheaf of holomorphic differentials on  $C$  and  $\gamma$  is any path from  $c_0$  to  $c$ . In a more algebraic interpretation, the abelian group  $J(\mathbb{C})$  is isomorphic to  $\text{Pic}^0(C)/C(C)^*$ , the group of degree zero divisors on  $C$  modulo principal divisors, and the map above is simply:

$$\begin{aligned} C(\mathbb{C}) &\rightarrow J(\mathbb{C}) \\ c &\mapsto c - c_0. \end{aligned}$$

This construction can be carried out over any field  $k$ , provided  $C(k) \neq \emptyset$  and also contains the basepoint  $c_0$ : by a fundamental result of Weil, the Jacobian  $J$

is defined over the field of definition of  $C$ , and the set-theoretic maps above arise from  $k$ -morphisms.

For each  $n \in \mathbb{N}$ , we get maps

$$C^n(k) \xrightarrow{\sigma_n} C^{(n)}(k) \xrightarrow{\varphi_n} J(k)$$

where  $C^n$  is the  $n$ -th power and  $C^{(n)} = C^n/\mathfrak{S}_n$  is the  $n$ -th symmetric power of  $C$ , i.e.,  $C^{(n)}(k)$  is the set of effective degree  $n$  zero-cycles on  $C$  which are defined over  $k$ . The map to the Jacobian assigns to a degree  $n$  zero-cycle  $c_1 + \dots + c_n \in C^{(n)}(k)$  the degree 0 zero-cycle  $(c_1 + \dots + c_n) - nc_0$ . The maps  $\varphi_n$  capture interesting geometric information. For example,  $\varphi_g$  is birational, which leads to an alternative definition of  $J$  as the unique abelian variety birational to  $C^{(g)}$ . The locus  $\Theta := \varphi_{g-1}(C^{(g-1)}) \subset J$  is an ample divisor, the theta-divisor. The classical Torelli theorem says that the pair  $(J, \Theta)$ , consisting of the Jacobian  $J$  of  $C$  and its polarization  $\Theta$ , determines  $C$  up to isomorphism. This theorem holds over any field and is one of the main tools in geometric and arithmetic investigations of algebraic curves, relating these to much more symmetric objects - abelian varieties.

From now on, let  $k_0$  be a finite field of characteristic  $p$  and  $k = \bar{k}_0$  an algebraic closure of  $k_0$ . Recall that  $J(k)$  is a torsion abelian group, with  $\ell$ -primary part

$$J\{\ell\} \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}, \quad \text{for } \ell \neq p.$$

The description of  $J\{p\}$  is slightly more complicated: there exists a nonnegative integer  $n \leq g$  such that  $J\{p\} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^n$ . Nevertheless, as an abstract abelian group,  $J(k)$  depends “almost” only on the genus  $g$  of  $C$ . The procyclic Galois group of  $k/k_0$  acts on  $J(k)$  and one can consider the Galois representation on the Tate-module:

$$T_\ell(J) := \varprojlim J[\ell^n], \quad \ell \neq p,$$

where  $J[\ell^n] \subset J(k)$  is the subgroup of  $\ell^n$ -torsion points. Let  $F_J$  be the characteristic polynomial of the Frobenius endomorphism on

$$V_\ell(J) := T_\ell(J) \otimes \mathbb{Q}_\ell.$$

By a fundamental result of Tate,  $F_J$  determines the Jacobian as an algebraic variety, modulo isogenies:

**Theorem 1.1** (Tate [Tat66]). *Let  $J, \tilde{J}$  be abelian varieties over  $k_0$  and  $F_J, F_{\tilde{J}} \in \mathbb{Z}[T]$  the characteristic polynomials of the  $k_0$ -Frobenius endomorphism  $\text{Fr}$  acting on  $V_\ell(J)$ , resp.  $V_\ell(\tilde{J})$ . Then*

$$\text{Hom}(J, \tilde{J}) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \text{Hom}_{\mathbb{Z}_\ell[\text{Fr}]}(T_\ell(J), T_\ell(\tilde{J})).$$

*The abelian varieties  $J$  and  $\tilde{J}$  are isogenous if and only if  $F_J = F_{\tilde{J}}$ .*

In particular, while the Galois-module structure of  $J(k)$  distinguishes  $J$  in a rather strong sense (but not up to isomorphism of abelian varieties, an example can be found in [Zar], Section 12), the group structure of  $J(k)$  does not.

In this paper, we investigate a certain “group-theoretic” analog of the Torelli theorem for curves over *finite* fields. This analog has a natural setting in the anabelian geometry of curves. Throughout, we work in characteristic  $\geq 3$ .

Let  $J^1 = J^1$  be the Jacobian of (degree 1 zero-cycles of)  $C$  and

$$\begin{array}{ccc} j_1 : C(k) & \hookrightarrow & J^1(k) \\ c & \mapsto & [c] \end{array} \quad (1)$$

the corresponding embedding. The Jacobian  $J$  of degree 0 zero-cycles on  $C$  acts on  $J^1$ , translating by points  $c \in C(k)$ . Let  $\tilde{C}$ , resp.  $\tilde{J}$ , be another smooth projective curve, resp. its Jacobian. We will say that

$$\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$$

is an isomorphism of pairs if there exists a diagram

$$\begin{array}{ccccc} J(k) & & J^1(k) & \xleftarrow{j_1} & C(k) \\ \phi^0 \downarrow & & \phi^1 \downarrow & & \downarrow \phi_s \\ \tilde{J}(k) & & \tilde{J}^1(k) & \xleftarrow{\tilde{j}_1} & \tilde{C}(k) \end{array}$$

where

- $\phi^0$  is an isomorphism of abstract abelian groups;
- $\phi^1$  is an isomorphism of homogeneous spaces, compatible with  $\phi^0$ ;
- the restriction  $\phi_s : C(k) \rightarrow \tilde{C}(k)$  of  $\phi^1$  is a bijection of sets.

Our main result is:

**Theorem 1.2.** *Let  $k = \bar{\mathbb{F}}_p$ , with  $p \geq 3$ , and let  $C, \tilde{C}$  be smooth projective curves over  $k$  of genus  $\geq 2$ , with Jacobians  $J$ , resp.  $\tilde{J}$ . Let*

$$\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$$

*be an isomorphism of pairs. Then  $J$  and  $\tilde{J}$  are isogenous.*

**Conjecture 1.3.** *Under the assumptions of Theorem 1.2,  $C$  and  $\tilde{C}$  are isomorphic as algebraic varieties, modulo Frobenius twisting.*

There are examples of geometrically nonisomorphic curves over finite fields with isomorphic Jacobians, as (unpolarized) algebraic varieties over  $k_0$ . Pairs of such curves are given by

$$y^2 = (x^3 + 1)(x^3 - 1) \text{ and } y^2 = (x^3 - 1)(x^3 - 4)$$

over  $\mathbb{F}_{11}$  with Jacobian  $E \times E$ , for a supersingular elliptic curve  $E$ , or

$$y^2 = x^5 + x^3 + x^2 - x - 1 \text{ and } y^2 = x^5 - x^3 + x^2 - x - 1$$

over  $\mathbb{F}_3$ , with a geometrically simple Jacobian (see [IKO86], [How96] and the references therein).

Theorem 1.2 was motivated by Grothendieck's anabelian geometry. This is a program relating algebraic fundamental groups of hyperbolic varieties over arithmetic fields to the underlying algebraic structure. One of the recent theorems in this direction is due to A. Tamagawa: Let  $\Pi$  be a *nonabelian* profinite group. Then there are at most finitely many curves over  $k = \bar{\mathbb{F}}_p$  with tame fundamental group isomorphic to  $\Pi$  [Tam04]. Tamagawa generalized previous results by Pop-Saidi [PS03] and Raynaud [Ray02], who proved similar statements under some technical restrictions on curves. The main new ingredient in Tamagawa's proof is a delicate geometric analysis of special loci in Jacobians.

In the second part of this paper, we apply Theorem 1.2 to a somewhat orthogonal problem. Namely, we focus on the prime to  $p$  part of the *abelianization* of the absolute Galois group of the function field of the curve, together with the set of valuation subgroups. Our main result (Theorem 9.3) is that for projective curves  $C$  over  $k$ , of genus  $g(C) > 4$ , the pair  $(\mathcal{G}_K^a, \mathcal{I})$ , consisting of the abelianization of the Galois group of  $K = k(C)$  and the set  $\mathcal{I} = \{I_\nu\}_\nu$  of procyclic subgroups  $I_\nu \subset \mathcal{G}_K^a$  corresponding to nontrivial valuations of  $K$ , determines the isogeny class of the Jacobian of  $C$ .

Here is a road-map of the paper. In Section 2, included as a motivation for Conjecture 1.3, we discuss certain subvarieties of moduli spaces of curves cut out by conditions on the order of zero-cycles of the form  $c - c'$  on  $C$  in the group  $J(k)$  (i.e., images of Hurwitz schemes and their intersections). Typically, very few such conditions suffice to determine  $C$ , up to a *finite* choice. In Section 3 we study the formal automorphism group  $G_C$  of the pair  $(C, J)$  and derive some of its basic properties. In Section 4 we collect several group-theoretic results about profinite groups which we apply in Section 5 to prove that any elements  $\gamma, \tilde{\gamma} \in G_C$  have the property that some integral powers  $\gamma^n, \tilde{\gamma}^{\tilde{n}}$  commute. We then prove that this holds for the Frobenius endomorphisms  $\phi^0(\text{Fr})$  and  $\tilde{\text{Fr}}$ , as elements in  $\text{End}_{\tilde{k}_0}(\tilde{J})$ , whenever we have an isomorphism of pairs  $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$ . In Section 6 we apply the theory of integer-valued linear recurrences as in [CZ02] to obtain a sufficient condition for isogeny of abelian varieties. In Section 7 we construct towers of degree 2 field extensions

$$k_0 \subset \dots \subset k_n \dots \subset k_\infty, \text{ resp. } \tilde{k}_0 \subset \dots \subset \tilde{k}_n \dots \subset \tilde{k}_\infty,$$

provide set-theoretic intrinsic definitions of  $J(k_n)$ , resp.  $\tilde{J}(\tilde{k}_n)$ , and establish that

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n), \text{ for all } n.$$

Combining Tate's theorem 1.1 with Theorem 6.3 we conclude that  $J$  and  $\tilde{J}$  are isogenous. In Sections 8 and 9 we discuss extensions and applications of Theorem 1.2 to anabelian geometry. In the Appendix we establish several geometric facts on abelian subvarieties in special loci in Jacobians, needed in Section 9.

**Acknowledgments:** We are grateful to A. Venkatesh and U. Zannier for useful suggestions, and to B. Hassett and Yu. Zarhin for their comments. The first author was partially supported by NSF grant DMS-0701578. The third author was partially supported by NSF grant DMS-0602333.

## 2. Curves and their moduli

Let  $C$  be an irreducible smooth projective curve of genus  $g = g(C) > 1$  over a finite field  $k_0$  of characteristic  $p$ , with  $C(k_0) \neq \emptyset$ , and let  $J = J_C$  be its Jacobian. The Jacobian of degree 1 zero-cycles  $J^1$  is a principal homogeneous space for  $J$ . For  $\ell$  a prime number let

$$J\{\ell\} := \cup_{n \in \mathbb{N}} J[\ell^n] \subset J(k), \quad \text{resp.} \quad T_\ell(J) = \varprojlim J[\ell^n]$$

be the  $\ell$ -primary part of  $J(k)$ , resp. the Tate-module. For any set of primes  $S$ , put

$$J\{S\} := \bigoplus_{\ell \in S} J\{\ell\} \subset J(k).$$

The order of  $x \in J(k)$  will be denoted by  $\text{ord}(x)$ .

**Lemma 2.1.** Let  $C$  be a curve of genus  $g > 1$ . Let  $J$  be its Jacobian and  $a \in J(k)$  be such that

$$a + C(k) \subset C(k) \subset J^1(k).$$

Then  $a = 0$ .

*Proof.* Let  $\langle a \rangle$  be the cyclic subgroup generated by  $a$  and let  $n$  be its order. The translation by  $a$  gives an action of  $\langle a \rangle$  on  $J^1$  and a separable nonramified covering  $C \rightarrow C/\langle a \rangle$  of degree  $n$ . The quotient  $\bar{J} := J/\langle a \rangle$  acts on the corresponding principal homogeneous space  $\bar{J}^1 = J^1/\langle a \rangle$ . The image  $\bar{C}$  of  $C$  under the projection  $J^1 \rightarrow \bar{J}^1$  has genus  $\bar{g} = g/n - 1/n + 1 < g$ , since  $n \geq 2$  and  $g(C) \geq 2$ . Hence the Jacobian of  $\bar{C}$  is a proper abelian subvariety of  $\bar{J}$ , of dimension at most  $\bar{g}$ . It follows that the same holds for its preimage  $C$ , contradicting the fact that  $C$  generates  $J$ .  $\square$

**Definition 2.2.** A ordered set  $R_n = \{r_1, \dots, r_n\}$  of integers  $r_j > 1$ , with  $p \nmid r_j$  for all  $j$ , will be called an  $n$ -string. Let  $J$  be an abelian variety over  $k$  and  $X \subset J(k)$ . A ordered subset  $\{x_0, x_1, \dots, x_n\} \subset X$  will be called an  $R_n$ -configuration on  $X$  if  $r_j = \text{ord}(x_j - x_0)$ , for  $1 \leq j \leq n$ .

We will mostly consider the case when  $X = C(k) \hookrightarrow J(k)$ , where  $C$  is a curve of genus  $g = g(C) \geq 1$ . Note that an isomorphism of pairs  $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$  preserves all configurations, i.e., for all  $n \in \mathbb{N}$ , every  $R_n$ -configuration in  $C(k) \subset J(k)$  is mapped to an  $R_n$ -configuration in  $\tilde{C}(k) \subset \tilde{J}(k)$ .

**Theorem 2.3.** *Let  $C$  be a curve over  $k = \bar{\mathbb{F}}_p$  of genus  $g > 1$ . Then there exists a string  $R_n$ , with  $n < 2g$  such that*

- $C(k) \subset J(k)$  contains an  $R_n$ -configuration,
- there exist at most finitely many nonisomorphic curves of genus  $g$  containing an  $R_n$ -configuration, modulo Frobenius twists.

*Proof.* We write  $\mathcal{M}_{g,n}$  for the moduli space (stack) of genus  $g$  curves with  $n$ -marked points. We start with the following

**Lemma 2.4.** Every string  $R_1$  defines an algebraic subvariety  $\mathcal{D}_{R_1,g} \subset \mathcal{M}_{g,1}$  of dimension  $2g - 1$  with a finite surjection onto a subvariety of  $\mathcal{M}_g$ .

*Proof.* Moduli computation. The cycle  $c_1 - c_0$  of order  $m$  prime to  $p$  is the same as a function  $f$  on  $C$  with divisor  $m(c_1 - c_0)$ . It defines a separable cover  $C \rightarrow \mathbb{P}^1$  of degree  $m$ , which is completely ramified over two points:  $0, \infty$ . The variety of such covers is a Hurwitz scheme, it is defined over  $\mathbb{F}_p \subset k$ . The genus computation gives an upper bound of  $2g$  for the number of additional ramification points. Since there are only finitely many covers of fixed degree with fixed branch points in  $\mathbb{P}^1$ , the dimension of the corresponding Hurwitz scheme is bounded by  $2g - 1$ .  $\square$

**Remark 2.5.** Over  $\mathbb{C}$ , this Hurwitz scheme is irreducible and has dimension  $2g - 1$ . The generic point of this scheme corresponds to a cover with simple additional ramification points whose images are all distinct.

The subvariety of  $\mathcal{M}_g$  parametrizing curves with an  $R_n$ -configuration is contained in the intersection of varieties corresponding to configurations of order 1 built from appropriate subsets of  $R_n$ .

We proceed by induction: Assume that  $C$  contains an  $R_n$ -configuration  $\{c_0, \dots, c_n\} \subset C(k)$  and let  $\mathcal{D}_{R_n} \subset \mathcal{M}_{g,1}$  be a union of irreducible subvarieties of dimension  $2g - n - 1$ , corresponding to curves with such a configuration, each having a finite map onto a subvariety of  $\mathcal{M}_g$ . We will use Hrushovski's theorem [Hru96] for the Jacobian fibration of the universal curve over the function field of each irreducible component  $\mathcal{D}$  of  $\mathcal{D}_{R_n}$ : the number of points of finite order (coprime to  $p$ ) on a nonisotrivial curve embedded into an abelian variety, over a function field of positive dimension, is bounded. In particular, there exists an  $N_{n+1}$  such that:

1. there is a point  $c_{n+1}$  with  $c_{n+1} - c_0$  of order  $N_{n+1}$ ,
2. the subvariety of  $\mathcal{D}$  parametrizing curves with a torsion point of order  $N_{n+1}$  is a proper subvariety.

Iterating this, in at most  $2g - 1$  steps we obtain a string  $R$  and a zero-dimensional variety  $\mathcal{D}$  such that  $C(k)$  contains an  $R$ -configuration which distinguishes  $C$  from all but finitely many other genus  $g$  curves over  $k$ .

Note that the presence of a given configuration is invariant under Galois automorphisms. Since the subvarieties  $\mathcal{D} \subset \mathcal{M}_{g,1}$  are defined over  $k_0$  we obtain in the end a subset of  $k_0$ -points in  $\mathcal{M}_{g,1}$ .  $\square$

Theorem 2.3 is far from optimal. If we assume that  $c_0$  is defined over  $k_0$  and  $c_1$  over an extension of  $k_0$  than the Galois conjugate of  $c_1 - c_0$  has the same order, so that the corresponding point in the image of the Hurwitz scheme in  $\mathcal{M}_{g,1}$  is singular and, moreover, nonnormal.

We have  $\dim \mathcal{M}_{g,1} = 3g - 2$  and  $\text{codim } \mathcal{D}_n = g - 1$ . If the varieties  $\mathcal{D}_n$  intersected with correct codimensions then a 3-configuration would give a subvariety of dimension 1 in  $\mathcal{M}_{g,1}$  and a 4-configuration - a zero-dimensional subvariety in  $\mathcal{M}_{g,1}$ .

By generic local computations, the dimension of double and triple intersections of Hurwitz schemes corresponding to 1-strings with coprime entries should be at most the dimension of a transversal intersection of varieties of the same dimension. Thus we expect that a triple intersection has dimension 1, and that quadruple intersections have dimension 0.

**Conjecture 2.6.** *For any curve  $C$  of genus  $g(C) \geq 2$  there exist a string  $R_4$  and an  $R_4$ -configuration on  $C$  such that all curves  $\tilde{C}$  with an  $R_4$ -configuration on  $\tilde{C}$  realizing the  $R_4$ -string are Galois conjugated to  $C$ . Moreover, all such configurations on  $C$  are also Galois conjugated.*

Clearly, this would imply a strong version of Conjecture 1.3.

**Remark 2.7.** Consider  $R_3 = \{2, 3\}$ . Transversality would give  $3g - 2 - (2g - 2) = g$  in this case. However, the corresponding intersection is trivial.

Indeed, in general the set of solutions  $nc_0 = nc$  is trivial for odd  $n \leq g - 1$ , and a point  $c_0$  invariant under a hyperelliptic involution. For  $n \leq g - 1$  and  $n$  even the point  $c$  is always invariant under a hyperelliptic involution.

In fact, we have a “supertransversality” for these Hurwitz schemes.

**Proposition 2.8.** *Let  $r_1, r'_1$  be coprime integers. Let  $R_1 = \{r_1\}$  and  $R'_1 = \{r'_1\}$  be the corresponding 1-strings and  $\mathcal{Z} := \mathcal{D}_{R_1, g} \cap \mathcal{D}_{R'_1, g} \subset \mathcal{M}_{g,1}$  the intersection of the associated Hurwitz schemes. Then  $\mathcal{Z} = \emptyset$ , provided  $g \geq (r_1 - 1)(r'_1 - 1)/2$ .*

*Proof.* The coprimality condition implies that the pair of functions  $(f_{r_1}, f_{r'_1})$ , with divisors  $r_1(c_1 - c_0)$ , resp.  $r'_1(c'_1 - c_0)$ , realizing the configuration, gives a map  $C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ , birational onto its image. The family of such curves in  $\mathbb{P}^1 \times \mathbb{P}^1$  is algebraic. Hence  $g(C) \leq (r_1 - 1)(r'_1 - 1)/2$ . A smooth curve in the family has genus  $g = (C(C + K)/2) + 1$  (where  $K = K_{\mathbb{P}^1 \times \mathbb{P}^1}$  is the canonical class) which gives

$$(r_1 H + r'_1 H')((r'_1 - 2)H + (r'_1 - 2)H') = (2r_1 r'_1 - 2r_1 - 2r'_1)/2 + 1 = (r_1 - 1)(r'_1 - 1).$$

The image of  $C$  in  $\mathbb{P}^1 \times \mathbb{P}^1$  has a singularity in the image of  $c_0$ , the same singularity as the rational curve  $(t^{r_1}, t^{r'_1})$ . This rational curve has the same homology class as  $C$  and has exactly two equivalent singularities, at  $(0, 0)$  and at  $(\infty, \infty)$ . Thus

if  $(r_1 - 1)(r'_1 - 1) - 2\delta(r_1, r'_1) = 0$  then the defect of the singularity is  $\delta(r_1, r'_1) = (r_1 - 1)(r'_1 - 1)/2$ , which gives a lower bound for the defect for  $C$ . Hence  $\mathbf{g}(C) \leq (r_1 - 1)(r'_1 - 1)/2$ .  $\square$

**Conjecture 2.9.** *Let  $f_{r_1}, f_{r'_1}, f_{r''_1} \in k(C)$  be functions as above and  $\lambda \in k^* \setminus \{1\}$ . Assume that there are four points  $c_0, c_1, c_2, c_3 \in C(k)$  such that*

$$\begin{aligned}\operatorname{div}(f_{r_1}) &= r_1(c_0 - c_1) \\ \operatorname{div}(f_{r'_1}) &= r'_1(c_0 - c_2) \\ \operatorname{div}(f_{r''_1}) &= r''_1(c_0 - c_3)\end{aligned}$$

and such that

$$f_{r_1}(c_2) = 1 \text{ and } f_{r_1}(c_3) = \lambda.$$

Then there are only finitely many curves  $\tilde{C}$  with the same property.

This would imply that the 3-point scheme intersection

$$\mathcal{D}_{R_1, \mathbf{g}} \cap \mathcal{D}_{R'_1, \mathbf{g}} \cap \mathcal{D}_{R''_1, \mathbf{g}} \subset \mathcal{M}_{\mathbf{g}, 1}$$

has dimension at most 1, and consequently the finiteness part of Conjecture 2.6. We don't know whether or not this intersection is irreducible. We would expect it at least for sufficiently large coprime  $r_1, r'_1, r''_1$ .

### 3. Formal automorphisms

Let  $A$  be an abelian variety,  $A^1$  a principal homogeneous space for  $A$  and  $X \subset A^1$  a subvariety not preserved by the action of an abelian subvariety of  $A$  of positive dimension.

**Lemma 3.1.** The subgroup

$$\operatorname{Stab}_X := \{a \in A(k) \mid a + X(k) \subset X(k)\}$$

is finite.

*Proof.* See, e.g., [Abr94].  $\square$

Let  $\operatorname{Aut}(A)$  be the group of automorphisms of the torsion abelian group  $A(k)$ . Note that  $\operatorname{Aut}(A)$  is a profinite group since all of its orbits in  $A(k)$  are finite. In fact, we have

$$\operatorname{Aut}(A) = \operatorname{Aut}(A)_p \times \prod_{\ell \neq p} \operatorname{GL}_{2d}(\mathbb{Z}_\ell),$$

with  $d = \dim A$  and  $\operatorname{Aut}(A)_p = \operatorname{GL}_n(\mathbb{Z}_p)$ , where  $n$  is the rank of the étale  $p$ -subgroup of  $A(k)$ .



The group  $\text{Aut}(A)$  has a split affine extension

$$1 \rightarrow A(k) \rightarrow \text{Aut}(A)^{\text{aff}} \rightarrow \text{Aut}(A) \rightarrow 1 \quad (2)$$

which acts on  $A^1(k)$ . Since  $A(k)$  is a discrete group,  $\text{Aut}(A)^{\text{aff}}$  carries a natural topology. Let

$$G_X := \{\gamma \in \text{Aut}(A)^{\text{aff}} \mid \gamma(X(k)) \subseteq X(k) \subset A^1(k)\}$$

be the subgroup preserving  $X(k)$ . We call  $G_X$  the group of automorphisms of the pair  $(X, A)$ .

**Lemma 3.2.** The group  $G_X$  is closed in the topological group  $\text{Aut}(A)^{\text{aff}}$ . Its projection to  $\text{Aut}(A)$  has finite kernel.

*Proof.* Choose a point  $x \in X(k) \subset A^1(k)$  and let  $\text{Aut}(A)_x \subset \text{Aut}(A)^{\text{aff}}$  be a section of the projection in (2) of automorphisms fixing  $x$ . With this choice, we may assume that  $X \subset A$ . We claim that the subgroup  $G_X \cap \text{Aut}(A)_x$  has finite index in  $G_X$ , for all  $x \in X$ , and that its image in  $\text{Aut}(A)_x$  is closed in the profinite topology.

For each  $\alpha \in A(k)$  the stabilizer  $G_\alpha \subset G_X$  has finite index since the order of  $\alpha$  is unchanged under an automorphism of  $X$ . Note that  $G_X$  acts on the subgroup of  $A(k)$  generated by zero-cycles with support in  $X(k)$ . Consider the map

$$\begin{aligned} X \times X &\rightarrow A \\ (x, x') &\mapsto x - x', \end{aligned}$$

choose an  $\alpha \in A(k)$  whose preimage in  $X \times X$  is nonempty and of minimal dimension and let  $X_\alpha$  be the projection of this preimage to the first factor. Note that the stabilizer  $G_\alpha$  preserves  $X_\alpha(k)$  and that for dimension reasons  $\dim X_\alpha < \dim X$ . Thus we can assume that  $G_\alpha$  maps to  $G_{X_\alpha}$ . If  $\dim X_\alpha = 0$  then  $G_X \cap \text{Aut}(A)_x$  has finite index in  $G_\alpha$  (and hence in  $G_X$ ) for any  $x \in X_\alpha(k)$ . There are two possibilities:

1.  $X_\alpha$  is not preserved by the action of a nontrivial proper abelian subvariety of  $A$ ,
2.  $X_\alpha$  is preserved by the action of a nontrivial proper abelian subvariety  $B_\alpha \subset A$ .

In the first case we use induction on dimension: if  $\dim X_\alpha > 0$  then, by the inductive assumption, we can find an  $x \in X_\alpha(k)$  with  $G_{X_\alpha} \cap \text{Aut}(A)_x$  having finite index in  $G_{X_\alpha}$ . The preimage of  $G_{X_\alpha} \cap \text{Aut}(A)_x$  in  $G_\alpha$  has also finite index in  $G_X$  and we obtain the result.

In the second case,  $G_{X_\alpha}$  contains  $B_\alpha(k)$  as a subgroup and  $G_{X_\alpha}/B_\alpha(k)$  has a subgroup of finite index  $G_{X_\alpha}/B_\alpha(k) \cap \text{Aut}(A)_{x'}$ , by the inductive assumption. Thus  $G_X$  contains a subgroup  $G_{B_\alpha+x'}x$  of finite index. Consider other subvarieties  $G_{X'_\alpha}$ . Then either there exists an  $X'_\alpha$  which is not preserved by the action of an abelian subvariety and we can apply the previous argument to find a point  $x \in X'_\alpha(k)$  or there is a nontrivial  $B$  such that all  $X_\alpha$  are preserved by the action

of  $B$ . Since the union of all  $X_\alpha$  of minimal nonzero dimension forms an open subset of  $X$  we obtain that  $X$  is preserved by the action of  $B$ , contradicting our assumption. Thus we can find at least one  $x \in X(k)$  with  $G_X \cap \text{Aut}(A)_x$  of finite index in  $G_X$ . Note that for other  $x' \in X$  we have

$$G_X \cap \text{Aut}(A)_x \cap \text{Aut}(A)_{x'} = G_X \cap \text{Aut}(A)_x \cap G_{x-x'}$$

and hence it has finite index in  $G_X$ . It follows that  $G_X \cap \text{Aut}(A)_{x'}$  also has finite index in  $G_X$ , for any  $x' \in X(k)$ .

Thus the orbit  $G_X \cdot x$  is finite. The stabilizer of  $x$  in  $G_X$  has finite index and lies in  $\text{Aut}(A)_x$ . It remains to observe that the stabilizer is closed in  $\text{Aut}(X)_x$ , using the same argument.

Lemma 2.1 implies immediately that the projection has finite kernel.  $\square$

**Remark 3.3.** The group  $G_X$  always contains the procyclic subgroup  $\hat{\mathbb{Z}}$  generated by a Frobenius automorphism, and its extension by a finite group of algebraic automorphisms of the pair  $(X, A)$ .

**Proposition 3.4.** *Let  $A$  be an abelian variety of dimension  $d$  and  $X \subset A^1$  a subvariety. Let  $G_X$  be the group of automorphisms of the pair  $(X, A)$ . Let*

$$\psi = \prod_{\ell \neq p} \psi_\ell : G_X \rightarrow \prod_{\ell \neq p} \text{GL}_{2d}(\mathbb{Z}_\ell)$$

*be the corresponding homomorphism. Then, for all  $\gamma \in G_X, \gamma \neq 1$ , there are infinitely many  $\ell$  such that  $\psi_\ell(\gamma) \neq 1$ .*

*Proof.* Assume the contrary. Then there is a finite set of primes  $S$  and a projection  $X \rightarrow A\{S\}$  such that  $\gamma$  acts trivially on the fibers. Let  $y \in A\{S\}$  be such that  $y \neq \gamma(y)$  and let  $X_y$  be the preimage of  $y$  in  $X$ . Then  $\gamma(X_y) = X_{\gamma(y)}$ . Moreover,  $X_{\gamma(y)} = X_y + \gamma(x) - x$ . Thus  $X_{\gamma(y)} \subset X \cap (X + \gamma(x) - x)$ . On the other hand,  $X \cap (X + \gamma(x) - x)$  is a proper subvariety of smaller dimension.

However, the number of points in  $X$  and  $X_y$  is the same for finite fields over which the points from  $A\{S\}$  are not defined, and the number of such fields is infinite. Contradiction.  $\square$

**Definition 3.5.** *A homomorphism of abelian groups  $\phi^0 : A(k) \rightarrow A(k)$  is called a formal isogeny if it arises from a sequence  $\{\phi_i^0\}$  of algebraic isogenies  $\phi_i^0 : A \rightarrow A$ , with the property that for all finite subgroups  $G \subset A(k)$ , there exists an  $n(G) \in \mathbb{N}$  such that  $\phi_i^0|_G = \phi_{i'}^0|_G$ , for all  $i, i' \geq n(G)$ .*

An example is a  $\hat{\mathbb{Z}}^*$ -power of the Frobenius endomorphism  $\text{Fr} \in \text{End}_{k_0}(A)$ .

**Proposition 3.6.** *Let  $(X, A)$  be a pair as in Proposition 3.4 and let  $\gamma \in G_X$  be an element which commutes with the Frobenius action. Then  $\gamma$  is a formal isogeny.*

*Proof.* By Tate's theorem 1.1,  $\text{End}_{k_0}(A) \otimes \mathbb{Z}_\ell$  is equal to the centralizer of Frobenius in  $\text{End}(T_\ell)$ . By assumption, the reduction of  $\psi_\ell(\gamma)$  is in this centralizer, modulo any finite power of  $\ell$ . Thus it is approximated by elements in  $\text{End}_{k_0}(A)$ , on every finite subgroup of  $A(k)$ .  $\square$

#### 4. Group-theoretic background

In this section we collect some group-theoretic facts which will be needed in the proof of Theorem 5.13 - assuring that the Frobenius endomorphisms in  $\text{End}_k(J) = \text{End}_k(\tilde{J})$  commute.

**Lemma 4.1.** Let  $\ell > n + 1$  be a prime and  $G \subset \text{GL}_n(\mathbb{Z}_\ell)$  a closed subgroup with an abelian  $\ell$ -Sylow subgroup. Assume further that  $G$  is generated by its  $\ell$ -Sylow subgroups. Then  $G$  is abelian.

*Proof.* Since  $\ell > n + 1$ , the group  $G$  does not contain elements of finite  $\ell$ -order. Indeed, assume that  $\gamma \in \text{GL}_n(\mathbb{Z}_\ell)$  has order  $\ell$ . Then it generates a subalgebra of the matrix algebra which contains a subfield  $\mathbb{Q}_\ell(\sqrt[\ell]{1})$ , which has dimension  $\ell - 1$  over  $\mathbb{Q}_\ell$ , and has to embed into the natural representation space  $\mathbb{Q}_\ell^n$ . This implies that  $\ell \leq n + 1$ .

Consider the reduction homomorphism

$$\bar{\psi}_\ell : G \rightarrow \text{GL}_n(\mathbb{Z}/\ell).$$

The preimage  $G^0 = \bar{\psi}_\ell^{-1}(1)$  of the identity in  $\text{GL}_n(\mathbb{Z}/\ell)$  is a normal pro- $\ell$  subgroup. In particular,  $G_0$  is contained in every  $\ell$ -Sylow subgroup of  $G$ . Hence  $G_0$  is abelian and torsion-free, i.e.,  $G_0 \simeq \mathbb{Z}_\ell^r$ , for some  $r \in \mathbb{N}$ .

*Step 1.* Since  $G$  is generated by its  $\ell$ -Sylow subgroups, which are abelian, and  $G_0$  is contained in all these subgroups,  $G_0$  commutes with all elements of  $G$ . Let  $G'_0$  be the  $\ell$ -component of the center of  $G$ . It is a torsion free group isomorphic to  $\mathbb{Z}_\ell^r$  and containing  $G_0$  as a subgroup of finite index.

Thus  $G$  is a central extension

$$1 \rightarrow G'_0 \rightarrow G \rightarrow G' \rightarrow 1 \tag{3}$$

where  $G'$  is a finite group.

*Step 2.* This central extension is defined by an element  $\gamma \in H^2(G', \mathbb{Z}_\ell)$ , which has finite order since  $G'$  is finite. Hence  $\gamma$  is the image of an element from  $H^1(G', \mathbb{Z}/\ell^m)$  for some  $m \in \mathbb{N}$ , under the Bockstein homomorphism. This means that the corresponding central extension is induced from a homomorphism  $G' \rightarrow (\mathbb{Z}/\ell^m)^r$ , i.e., we have a commutative diagram

$$\begin{array}{ccccccc}
& & & \tilde{G} & \xlongequal{\quad} & \tilde{G} & \\
& & & \downarrow & & \downarrow & \\
1 & \longrightarrow & G'_0 & \longrightarrow & G & \longrightarrow & G' \longrightarrow 1 \\
& & \downarrow & & \downarrow f & & \downarrow \\
1 & \longrightarrow & \mathbb{Z}_\ell^r & \longrightarrow & \mathbb{Z}_\ell^r & \longrightarrow & (\mathbb{Z}/\ell^m)^r \longrightarrow 1 \\
& & & & \downarrow & & \downarrow \\
& & & & 1 & & 1
\end{array},$$

where  $\tilde{G} = \text{Ker}(f)$  is a finite normal subgroup of  $G$ .

*Step 3.* Since  $G$  has no  $\ell$ -torsion,  $\tilde{G}$  has order coprime to  $\ell$ . It follows that  $f$  admits a section  $\sigma : \mathbb{Z}_\ell^r \rightarrow G$ .

*Step 4.* We claim that  $\mathbb{Z}_\ell^r$  acts trivially on  $\tilde{G}$  and that the extension

$$1 \rightarrow \tilde{G} \rightarrow G \xrightarrow{f} \mathbb{Z}_\ell^r \rightarrow 1$$

splits.

Let  $g \in \text{GL}_n(\mathbb{Z}_\ell)$  be an element of infinite  $\ell$ -order (i.e., all reductions  $\bar{\psi}_{\ell^m}(g) \in \text{GL}_n(\mathbb{Z}/\ell^m)$  are of nontrivial  $\ell$ -power order). Consider an element  $h \in G \subset \text{GL}_n(\mathbb{Z}_\ell)$  of finite order. Assume that  $g^\ell$  commutes with  $h$ . Then  $g$  commutes with  $h$ .

We have  $g = g_s g_u$  where  $g_s$  is semi-simple,  $g_u$  is unipotent, and  $g_s, g_u$  commute. If an element  $h \in \text{GL}_n(\mathbb{Z}_\ell)$  has finite order and commutes with  $g$  then it commutes with  $g_s$  and  $g_u$ . Note that  $g_u^\ell = (g_u)^\ell$  and that they have the same commutators. Thus we can assume  $g = g_s$ . In this case the algebra  $\mathbb{Q}_\ell[g] \subset \text{Mat}_{n \times n}(\mathbb{Q}_\ell)$  is a direct sum of fields  $K_i^{(g)}$  (finite extensions of  $\mathbb{Q}_\ell$ ).

The subalgebra in  $\text{Mat}_{n \times n}(\mathbb{Q}_\ell)$  of elements commuting with  $h$  is a direct sum of matrix algebras over division algebras with centers  $K_i^{(g)}$ . We have a natural embedding of algebras  $\mathbb{Q}_\ell[g^\ell] \subseteq \mathbb{Q}_\ell[g]$ . If this embedding is an isomorphism then  $h$  commutes with  $g$ . Otherwise, there is a proper subfield  $K_i^{(g^\ell)} \subset K_i^{(g)}$ , which does not contain the projection of  $g$  to this component of the matrix algebra. Since it contains  $g^\ell$ , the corresponding extension has degree  $\ell$ , contradicting the assumption that  $\ell > n$ .

*Step 5.* Since  $G$  is generated by its  $\ell$ -Sylow subgroups and all elements of  $\tilde{G}$  commute with  $\mathbb{Z}_\ell^r$ , it follows that  $\tilde{G} = 1$  and  $G = \mathbb{Z}_\ell^r$ .  $\square$

**Lemma 4.2.** Let  $H' \rightarrow H$  be a surjective homomorphism of finite groups. Assume that we have an exact sequence

$$1 \rightarrow S_\ell \rightarrow H \rightarrow C \rightarrow 1$$

where  $S_\ell$  is a nontrivial normal  $\ell$ -subgroup of  $H$ ,  $C$  is a cyclic group whose order is a power of a prime number  $\neq \ell$ .

Then there is an  $\ell$ -Sylow subgroup  $S'_\ell \subset H'$  such that

- $S'_\ell$  surjects onto  $S_\ell$ ,
- the normalizer  $N'$  of  $S'_\ell$  in  $H'$  surjects onto  $H$ .

In particular, there exists an element  $h' \in N'$  of order coprime to  $\ell$  which surjects onto a generator of  $C$ .

*Proof.* All  $\ell$ -Sylow subgroups of  $H'$  surject onto  $S_\ell$ . Hence they generate a proper normal subgroup  $S' \subset H'$  which surjects onto  $S_\ell$ . Any  $h' \in H'$  acts (by conjugation) on the set  $\mathcal{S}(H')$  of  $\ell$ -Sylow subgroups of  $H'$ .

Since  $S'$  acts transitively on  $\mathcal{S}(H')$  there exists an element  $s' \in S'$  such that  $h's'$  acts with a fixed point on  $\mathcal{S}(H')$ . Let  $\tilde{S}'$  be an  $\ell$ -Sylow subgroup preserved by  $h's'$ . The normalizer  $N'$  of  $\tilde{S}'$  surjects onto  $H$ . In particular, we can find an element  $\tilde{h}'$  contained in this normalizer, of order coprime to  $\ell$ , which is mapped to a generator of  $C$ .  $\square$

Let  $H$  be a finite group and  $\ell, p$  two distinct primes. We say that  $H$  contains an  $(\ell, p^m)$ -extension  $\{s \in S_\ell, n \in N\}$  if the following holds:

- $S_\ell \subset H$  is an  $\ell$ -Sylow subgroup,
- $N \subset H$  is a subgroup containing  $S_\ell$  as a normal subgroup,
- the quotient  $C := N/S_\ell$  is a cyclic group of order  $p^{m+1}$ ,
- $n \in N$  projects onto a generator of  $C$ ,
- $s \in S_\ell$  satisfies  $[s, n^{p^m}] \neq 1$  in  $S_\ell$ .

**Corollary 4.3.** *Let  $\pi : H' \rightarrow H$  be a surjective homomorphism of finite groups. Assume that  $H$  contains an  $(\ell, p^m)$ -extension  $\{s \in S_\ell, n \in N\}$ . Then  $H'$  contains an  $(\ell, p^{m'})$ -extension  $\{s' \in S'_\ell, n' \in N'\}$ . Moreover,*

- $m' \geq m$ ,
- $\pi(S'_\ell) = S_\ell$ ,
- $\pi(s') = s$ ,
- $\pi(n') = n$ .

*Proof.* We start with the exact sequence

$$1 \rightarrow S_\ell \rightarrow N \rightarrow C \rightarrow 1. \quad (4)$$

The full preimage of  $N$  in  $H'$  contains an  $\ell$ -Sylow subgroup  $S'_\ell$  of  $H'$ . By Lemma 4.2, the normalizer of  $S'_\ell$  in  $H'$  contains an element  $n'$  of order coprime to  $\ell$  such that  $\pi(n') = n$ , surjecting onto a generator of  $C$ . We may correct  $n'$  such that its order becomes a power of  $p$ . It is divisible by the order of  $C$ , i.e., it equals  $p^{m'+1}$ , with  $m' > m$ . Let  $N' \subset H'$  be the subgroup generated by  $S'_\ell$  and  $n'$ . Take  $s'$  to be any element in the preimage  $\pi^{-1}(s)$ . Then  $\{s' \in S'_\ell, n' \in N'\}$  is the required  $(\ell, p^{m'})$ -extension.  $\square$

Let  $G$  be a semi-simple linear algebraic group over  $\mathbb{Z}$ . We will use the following generalization of a theorem of Jordan:

**Theorem 4.4.** *Let  $k_0$  be a field with  $q = p^r$  elements. There exists an  $n = n(\mathbf{G}) \in \mathbb{N}$  such that every subgroup  $G \subset \mathbf{G}(k_0)$  with  $p \nmid |G|$  contains an abelian normal subgroup  $H \subset G$  with  $|G/H| \leq n$ .*

*Further, there exists an  $\ell_0 = \ell_0(\mathbf{G})$  such that for all primes  $\ell'$  and all primes  $\ell \geq \ell_0$  with  $\ell \neq \ell'$ , the  $\ell$ -Sylow subgroups of  $\mathbf{G}(\mathbb{Z}/\ell')$  and  $\mathbf{G}(\mathbb{Z}/\ell)$  are abelian.*

*Proof.* See [BF66], [Wei84].  $\square$

**Proposition 4.5.** *Let  $G$  be a profinite group. Let  $S$  be an infinite set of primes. Assume that  $G$  admits a continuous homomorphism*

$$\psi = \prod_{\ell \in S} \psi_\ell : G \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}/\ell).$$

*Assume that for all  $\gamma \in G$ ,  $\gamma \neq 1$  one has*

$$\psi_\ell(\gamma) \neq 1 \in \mathbf{G}(\mathbb{Z}/\ell) \tag{5}$$

*for infinitely many  $\ell \in S$  (i.e.,  $\gamma$  has infinite support). Then*

1. *the induced reduction map*

$$\bar{\psi} := \prod_{\ell \in S} \bar{\psi}_\ell : G \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}/\ell)$$

*is injective;*

2. *there exists an  $\ell_0 = \ell_0(\mathbf{G})$  such that for all primes  $\ell > \ell_0$  the  $\ell$ -Sylow subgroup of  $G$  is abelian;*
3. *there exist a normal closed abelian subgroup  $H \subset G$  and an  $n = n(\mathbf{G})$  such that  $G/H$  has exponent bounded by  $n$ , i.e., the order of every element in  $G/H$  is bounded by  $n$ .*

*Proof.* Put

$$K_\ell := \text{Ker}(\mathbf{G}(\mathbb{Z}/\ell) \rightarrow \mathbf{G}(\mathbb{Z}/\ell)).$$

We have an exact sequence

$$1 \rightarrow \prod_{\ell \in S} K_\ell \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}/\ell) \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}/\ell) \rightarrow 1$$

Our assumption implies that  $\psi$  is injective, and we get an injection of the kernel of the reduction  $\text{Ker}(\bar{\psi}) \hookrightarrow \prod_{\ell \in S} K_\ell$ . If we had a nontrivial  $\gamma \in \text{Ker}(\bar{\psi})$ , its image  $\psi(\gamma)$  would generate a nontrivial closed procyclic subgroup isomorphic to  $\prod_{\ell' \in S'} \mathbb{Z}/\ell' \subset \prod_{\ell \in S} K_\ell$ , for some infinite set  $S' \subset S$ . Thus, there would exist a nontrivial element  $\gamma_{\ell'} \in \text{Ker}(\bar{\psi})$  such that  $\psi_\ell(\gamma_{\ell'}) = 1$  for all  $\ell \neq \ell'$ , contradicting our assumption. This proves the first claim.

The second claim follows by combining the injectivity of

$$\prod_{\ell' \in S \setminus \ell} \psi_{\ell'} : G \rightarrow \prod_{\ell' \in S \setminus \ell} G(\mathbb{Z}/\ell')$$

with Theorem 4.4.

From now on, we assume that  $\ell > \ell_0$  so that the  $\ell$ -Sylow subgroup of  $G$  is abelian.

**Lemma 4.6.** There exists a constant  $\kappa = \kappa(G)$  such that for all  $\ell > \ell_0$ , there exists a normal abelian subgroup  $Z_\ell \subset \bar{\psi}_\ell(G)$  of index

$$[\bar{\psi}_\ell(G) : Z_\ell] \leq \kappa.$$

*Proof.* If the image  $\bar{\psi}_\ell(G) \subset G(\mathbb{Z}/\ell)$  does not contain elements of order  $\ell$  we can directly apply Theorem 4.4 to conclude that  $\bar{\psi}_\ell(G)$  contains a normal abelian subgroup of index  $\kappa(G) = n(G)$ .

We may now assume that the image does contain elements of order  $\ell$ . We claim that there do not exist  $\gamma, \gamma' \in G$  such that

- $\bar{\psi}_\ell(\gamma), \bar{\psi}_\ell(\gamma')$  have  $\ell$ -power order and
- $\bar{\psi}_\ell(\gamma), \bar{\psi}_\ell(\gamma')$  do not commute in  $G(\mathbb{Z}/\ell)$ .

Otherwise, both  $\psi_\ell(\gamma)$  and  $\psi_\ell(\gamma')$  are contained in some  $\ell$ -Sylow subgroups of  $G(\mathbb{Z}_\ell)$ , which are both abelian, by the assumption  $\ell > \ell_0$ . By Lemma 4.1, the subgroup of  $G(\mathbb{Z}_\ell)$  generated by these  $\ell$ -Sylow subgroups is abelian, contradicting the second assumption.

It follows that all elements of  $\ell$ -power order in  $\bar{\psi}_\ell(G)$  commute, so that the group  $\bar{S}_\ell$  generated by them is in fact the  $\ell$ -Sylow subgroup of  $\bar{\psi}_\ell(G)$ . It is abelian and normal. Consider the exact sequence

$$1 \rightarrow \bar{S}_\ell \rightarrow \bar{\psi}_\ell(G) \rightarrow U_\ell \rightarrow 1 \quad (6)$$

where  $U_\ell := \bar{\psi}_\ell(G)/\bar{S}_\ell$ . Since  $\ell \nmid |U_\ell|$  the sequence (6) admits a section and there is an embedding

$$U_\ell \hookrightarrow \bar{\psi}_\ell(G) \subset G(\mathbb{Z}/\ell).$$

We apply Theorem 4.4 to conclude that  $U_\ell$  has an abelian normal subgroup  $A_\ell \subset U_\ell$  with  $|U_\ell/A_\ell| \leq n(G)$ . We have the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \bar{S}_\ell & \longrightarrow & \bar{\psi}_\ell(G) & \longrightarrow & U_\ell \longrightarrow 1 \\ & & \parallel & & \uparrow & & \uparrow \\ 1 & \longrightarrow & \bar{S}_\ell & \longrightarrow & H_\ell & \longrightarrow & A_\ell \longrightarrow 1 \end{array}$$

where  $H_\ell$  is the full preimage of  $A_\ell$  in  $\bar{\psi}_\ell(G)$ . It is a normal subgroup of  $\bar{\psi}_\ell(G)$  with

$$|\bar{\psi}_\ell(G)/H_\ell| = |U_\ell/A_\ell| \leq n(G).$$

Let  $Z_\ell \subset H_\ell$  be the centralizer of  $\bar{S}_\ell$ , it is a normal abelian subgroup of  $H_\ell$ . Lemma 4.6 follows if we show that the index  $[H_\ell : Z_\ell]$  is bounded independently of  $\ell$ .

There is a section

$$\sigma : A_\ell \rightarrow \bar{\psi}_\ell(G) \subset G(\mathbb{Z}/\ell).$$

In particular, the finite abelian group  $A_\ell$  has at most  $n := \text{rank}(G)$  generators. Consider the conjugation action of  $A_\ell$  on  $\bar{S}_\ell$ . For  $\mathbf{a} \in A_\ell$  let  $C(\mathbf{a})$  be the cyclic subgroup generated by the image of  $\mathbf{a}$  in the group of outer automorphisms of  $\bar{S}_\ell$ . It suffices to show that for each of the  $\leq n$  generators of  $A_\ell$  the order  $|C(\mathbf{a})|$  is bounded independently of  $\ell$  and  $\mathbf{a}$ .

Let  $C_p(\mathbf{a}) \subset C(\mathbf{a})$  be the  $p$ -Sylow cyclic subgroup, with  $p^{m+1} = |C_p(\mathbf{a})|$ . We have an extension of abelian groups

$$1 \rightarrow \bar{S}_\ell \rightarrow N_\ell \rightarrow C_p(\mathbf{a}) \rightarrow 1. \quad (7)$$

We claim that the length of the orbits of  $\mathbf{c} \in C_p(\mathbf{a})$  on  $\bar{S}_\ell$  is universally bounded, provided that  $q := p^m$  and  $\ell$  are sufficiently large. More precisely, we have:

**Lemma 4.7.** There exists a constant  $n' = n'(G)$  such that for all  $\mathbf{a} \in A_\ell$ , all  $\mathbf{s} \in \bar{S}_\ell$  and all generators  $\mathbf{c}$  of  $C_p(\mathbf{a})$  the commutator

$$[\mathbf{s}, \mathbf{c}^q] = 1,$$

provided  $\ell, q := p^m \geq n'$ .

*Proof.* We will argue by contradiction. We have

$$G = \varprojlim_i G_i, \quad \text{where} \quad G_i := \prod_{j=1}^i \bar{\psi}_{\ell_j}(G),$$

$\{\ell_1, \ell_2, \dots\}$  is the set of primes, with  $\ell_1 = \ell$ , and the maps  $\pi_i : G_{i+1} \rightarrow G_i$  are the natural projections. Assume that

$$[\mathbf{s}, \mathbf{c}^q] = \mathbf{s}' \neq 1 \quad \text{in} \quad \bar{S}_\ell. \quad (8)$$

We apply Corollary 4.3 inductively to conclude that each of the groups  $G_i$  has an  $(\ell, p^{m_i})$ -extension

$$\{\mathbf{s}_i \in S_{\ell,i}, \mathbf{n}_i \in N_i\}.$$

More precisely, there is a sequence of groups  $S_{\ell,i} \subset G_i$  and elements  $\mathbf{s}_i, \mathbf{n}_i \in G_i$  with the following properties:

- $S_{\ell,i}$  is an  $\ell$ -Sylow subgroup of  $G_i$ ,
- $\mathbf{s}_i \in S_{\ell,i}$



- $\mathbf{n}_i$  is in the normalizer of  $\mathbf{S}_{\ell,i}$ ,
- $\mathbf{n}_i$  has order  $p^{m_i}$  with  $m_i \geq m$ ,
- $[\mathbf{s}_i, \mathbf{n}_i^{p^{m_i}}] \neq 1$ ,
- $\pi_i(\mathbf{S}_{\ell,i+1}) = \mathbf{S}_{\ell,i}$ ,  $\pi_{i+1}(\mathbf{s}_{i+1}) = \mathbf{s}_i$ ,  $\pi_i(\mathbf{i}_{i+1}) = \mathbf{n}_i$ , for all  $i$ .

The corresponding limits

$$\gamma_s = \varprojlim \mathbf{s}_i, \quad \gamma_c = \varprojlim \mathbf{c}_i \in G$$

have infinite support and don't commute. Thus there exists a prime number  $r > \ell, q$  (and  $\ell_0(\mathbf{G})$ ) such that

$$[\bar{\psi}_r(\gamma_s), \bar{\psi}_r(\gamma_c)] \neq 1.$$

Let  $i$  be sufficiently large so that the prime  $r$  is among the primes  $\ell_1, \dots, \ell_i$ . There is a natural projection

$$\bar{\psi}_r : G_i \rightarrow \bar{\psi}_r(G) \subset \mathbf{G}(\mathbb{Z}/r).$$

The  $\ell$ -Sylow subgroup  $\mathbf{S}_{\ell,i}$  surjects onto the  $\ell$ -Sylow subgroup of  $\bar{\psi}_r(G)$ , which is abelian by Theorem 4.4. Let

$$\bar{\mathbf{N}}_r \subset \bar{\psi}_r(G) \subset \mathbf{G}(\mathbb{Z}/r)$$

be the *nonabelian* group generated by  $\bar{\psi}_r(\gamma_s)$  and  $\bar{\psi}_r(\gamma_n)$ , i.e., by  $\bar{\psi}_r(\mathbf{s}_i)$  and  $\bar{\psi}_r(\mathbf{n}_i)$ . It fits into an exact sequence

$$1 \rightarrow \bar{\mathbf{S}}_{\ell,r} \rightarrow \bar{\mathbf{N}}_r \rightarrow \bar{\mathbf{A}}_r \rightarrow 1,$$

where  $\bar{\mathbf{S}}_{\ell,r}$  is an abelian group of  $\ell$ -power order,  $\bar{\mathbf{A}}_r$  a cyclic abelian group of order divisible by  $p^{m+1}$ ,  $p \neq \ell$ .

Since  $r \nmid |\bar{\mathbf{N}}_r|$  we can apply Theorem 4.4: Any subgroup of  $\mathbf{G}(\mathbb{Z}/r)$  of order coprime to  $r$  has a normal abelian subgroup of index bounded by some constant  $n(\mathbf{G})$ . However, any abelian normal subgroup of  $\bar{\mathbf{N}}_r$  has index  $\geq \min(\ell, q)$ . We obtain a contradiction, when  $\ell$  and  $q$  are  $\geq n(\mathbf{G})$ .  $\square$

This finishes the proof of Lemma 4.6.  $\square$

We complete the proof of Proposition 4.5. Indeed, put

$$\bar{H} := \prod_{\ell \in S} (\bar{\psi}_\ell(G) \cap \mathbf{Z}_\ell) \subset \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}/\ell).$$

This is a closed abelian normal subgroup of  $\psi(G) = \prod_{\ell \in S} \bar{\psi}_\ell(G)$ . Since  $\psi$  is an injection, the preimage  $H := \psi^{-1}(\bar{H})$  is a closed abelian normal subgroup of  $G$ . By Lemma 4.6,  $[\bar{\psi}_\ell(G) : \mathbf{Z}_\ell] \leq \kappa$ , for all  $\ell$ , the quotient  $G/H$  has exponent bounded by  $\kappa$ .  $\square$

## 5. Curves and their Jacobians

Let  $C$  be a smooth projective curve of genus  $g \geq 2$  over a field  $k$  and  $J^n$  the Jacobian of degree  $n$  zero-cycles, or alternatively, degree  $n$  line bundles on  $C$ , with the convention  $J = J^0$ . We have the diagram

$$\begin{array}{ccc} C^n & \xrightarrow{\sigma_n} & C^{(n)} \\ & & \downarrow \varphi_n \\ & & J^n. \end{array}$$

For any field  $k_0$  we denote by  $C^{(n)}(k_0)$  the set of  $k_0$ -points of the variety  $C^{(n)}$ , i.e., the set of effective cycles  $c_1 + \dots + c_n$  defined over  $k_0$ . We write  $C(k_0)^{(n)} \subset C^{(n)}(k_0)$  for the subset of cycles  $c_1 + \dots + c_n$  where *each*  $c_i$  is defined over  $k_0$ . Put

$$W_n^r(C) := \{[L] \in J^n \mid \dim H^0(C, L) \geq r + 1\}, \quad W_n(C) := W_n^0(C).$$

The map  $\varphi_n$  is surjective for  $n \geq g$ . For  $n = g$  there is a divisor  $D \subset J$  such that for all  $x \in J(k) \setminus D(k)$ , the fiber  $\varphi_n^{-1}(x)$  consists of one point. For  $n \geq 2g - 1$ , the map  $\varphi_n$  is a  $\mathbb{P}^{n-g}$ -bundle.

We may fix a point  $c_0 \in C(k_0)$  and the embedding

$$\begin{array}{ccc} C & \hookrightarrow & J \\ c & \mapsto & [c - c_0]. \end{array}$$

This allows us to identify  $J^n$  and  $J$ .

**Lemma 5.1.** Consider the exact sequence

$$1 \rightarrow \mathbb{Z}_\ell^n \rightarrow \mathbb{Q}_\ell^n \rightarrow (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^n \rightarrow 1.$$

Let  $M \in \text{End}(\mathbb{Z}_\ell)$  be an endomorphism which is contained in  $\text{GL}_n(\mathbb{Q}_\ell)$ . Consider the induced action

$$M : (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^n \rightarrow (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^n,$$

and let  $\text{Ker}(M)$  be the kernel of this map. Then there is a canonical isomorphism

$$\mathbb{Z}_\ell^n / M(\mathbb{Z}_\ell^n) \simeq \text{ker}(M).$$

*Proof.* Consider the module  $M^{-1}(\mathbb{Z}_\ell^n)/\mathbb{Z}_\ell^n$  as a submodule of  $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^n$ . It is equal to  $\text{Ker}(M)$ . On the other hand,  $M$  induces an isomorphism

$$M^{-1}(\mathbb{Z}_\ell^n)/\mathbb{Z}_\ell^n \simeq \mathbb{Z}_\ell^n / M(\mathbb{Z}_\ell^n).$$

□

The following lemma will be used in Section 7.

**Lemma 5.2.** Fix a prime number  $\ell \neq p$  and assume that  $J(k_0) \supset J[\ell]$ . Let  $k_1/k_0$  be a degree  $\ell$ -extension. Then

- $\frac{1}{\ell}J(k_0) \subset J(k_1)$ ,
- $J\{\ell\} \cap J(k_1) = \frac{1}{\ell}J(k_0) \cap J\{\ell\}$ .

*Proof.* Let  $\text{Fr}$  be the  $k_0$ -Frobenius automorphism of  $k$ . Its action on the Galois-module  $V_\ell = V_\ell(J)$  is semi-simple, and decomposes  $V_\ell = \oplus_i K_i$ , where  $K_i/\mathbb{Q}_\ell$  are finite extensions. Note that the eigenvalues of the Frobenius on  $V_\ell$  are not roots of 1 and hence  $\text{Fr}^\ell - 1$  is always an invertible endomorphism of  $V_\ell$ . The Tate-module  $T_\ell := T_\ell(J)$  contains a submodule  $T'_\ell$  of finite index which is preserved by the Galois-action and decomposes as  $T'_\ell = \oplus_i \mathfrak{o}_i$ , where  $\mathfrak{o}_i \subset K_i$  are the rings of integers. The maximal ideal of  $\mathfrak{o}_i$  will be denoted by  $\mathfrak{m}_i$ .

The Frobenius acts on  $\mathfrak{o}_i$  via multiplication with a unit  $a_i \in \mathfrak{o}_i^*$ . By assumption, it acts trivially on  $J[\ell]$ . Since every  $\mathfrak{o}_i$  is isomorphic to a primitive  $\text{Fr}$ -submodule of  $T_\ell$  we have  $a_i \equiv 1 \pmod{\ell}$ , for all  $i$ , where  $(\ell) \subset \mathfrak{o}_i$  is a power of the maximal ideal  $\mathfrak{m}_i$ . We can write

$$a_i = 1 + \ell^{m_i} \varpi^{h_i} \quad \text{for } m_i, h_i \in \mathbb{N},$$

where  $\varpi_i$  is a generator of  $\mathfrak{m}_i$ , and the ideal  $(\varpi^{h_i}) \supset (\ell)$ . It follows that

$$a_i^\ell = 1 + \ell^{m_i+1} \varpi^{h_i} \pmod{\ell^{m_i+1} \varpi^{h_i+1}}. \quad (9)$$

Consider the filtration

$$(\text{Fr}^\ell - \text{Id})T'_\ell \subset (\text{Fr} - \text{Id}) \subset T'_\ell$$

and a similar filtration

$$(\text{Fr}^\ell - \text{Id})T_\ell \subset (\text{Fr} - \text{Id}) \subset T_\ell.$$

Observe that

$$|(\text{Fr} - \text{Id})T_\ell / (\text{Fr}^\ell - \text{Id})T_\ell| = |(\text{Fr} - \text{Id})T'_\ell / (\text{Fr}^\ell - \text{Id})T'_\ell| = \ell^{2g},$$

where the first equality follows from the fact that  $T'_\ell \subset T_\ell$  is a submodule of finite index, and the second assertion follows from Equation 9. From the exact sequence

$$1 \rightarrow T_\ell \rightarrow V_\ell \rightarrow J\{\ell\} \rightarrow 1$$

we observe that  $(\text{Fr} - 1)T_\ell / (\text{Fr}^\ell - 1)T_\ell$  is canonically isomorphic to  $J\{\ell\}^{\text{Fr}^\ell} / J\{\ell\}^{\text{Fr}}$ , by Lemma 5.1. Note that  $J\{\ell\}^{\text{Fr}^\ell}$  contains  $\frac{1}{\ell}J\{\ell\}^{\text{Fr}}$ . Indeed, by our assumption  $J[\ell] \subset J\{\ell\}^{\text{Fr}}$ . If  $x \in J\{\ell\}^{\text{Fr}}$  then  $\ell \text{Fr}(\frac{x}{\ell}) = x$  and hence  $\text{Fr}(\frac{x}{\ell}) = \frac{x}{\ell} + x_0$ , where  $\ell x_0 = 0$ , so that  $x_0 \in J[\ell]$ . Iterating, we obtain that

$$\text{Fr}^\ell\left(\frac{x}{\ell}\right) = \frac{x}{\ell} + \ell x_0 = \frac{x}{\ell}, \quad \text{and} \quad \frac{x}{\ell} \in J\{\ell\}^{\text{Fr}^\ell}.$$

It follows that  $J\{\ell\}^{\text{Fr}^\ell}/J\{\ell\}^{\text{Fr}}$  contains a subgroup isomorphic to  $(\mathbb{Z}/\ell)^{2g}$ . This implies the second claim of the lemma. The first follows via the same argument applied to arbitrary  $x \in J(k_0)$ .  $\square$

**Lemma 5.3.** For  $n \geq 2g-1$ , a field  $k_0$  such that  $\#k_0$  is sufficiently large, any finite extension  $k_1/k_0$  and any point  $x \in J(k_1)$  there exist points  $y, z \in \mathbb{P}^{n-g}(k_1) = \varphi_n^{-1}(x)$  such that the fiber  $\sigma_n^{-1}(y)$  is irreducible as a cycle over  $k_1$  and  $\sigma_n^{-1}(z)$  is completely reducible over  $k_1$ .

*Proof.* Follows from the equidistribution theorem [Kat02], Theorem 9.4.4.  $\square$

**Corollary 5.4.** *We have*

$$J(k) = \cup_{\Phi \in \text{End}_k(J)} \Phi(C(k)),$$

and in fact

$$J(k) = \cup_{n \in \mathbb{N}} n \cdot C(k). \quad (10)$$

Moreover, there exists a finite extension  $k'_0/k_0$  such that  $C(k_1)$  generates  $J(k_1)$ , for all finite extensions  $k_1/k'_0$ .

*Proof.* The existence of a  $y$  as in Lemma 5.3 implies the first statement (see [BT05b], Corollary 2.4, and [BT05a], Theorem 1). The second follows from the existence of  $z$ .  $\square$

It will be useful to be able to bound indices of subgroups in  $J(k_1)$  generated by fewer points from  $C(k_1)$ . Assume that  $k_1/k_0$  is a finite extension with  $\#k_1 = q$  and such that  $C(k_1)$  generates  $J(k_1)$ . Write

$$\#J(k_1) = q^g(1 + \Delta_q) \quad \text{and} \quad \#C(k_1) = q(1 + \delta_q)$$

We know that  $\Delta_q, \delta_q = O(\frac{1}{\sqrt{q}})$ , the implied constant depending only on the genus  $g(C)$ . We may assume that  $q$  is such that

$$|\Delta_q|, |\delta_q| \leq 1/2. \quad (11)$$

**Lemma 5.5.** Let  $D \subset C(k_1)$  be a subset of points such that

$$D/\#C(k_1) \leq \epsilon_q.$$

Let  $H \subset J(k_1)$  be the subgroup generated by points in  $C(k_1) \setminus D$ . Then

$$I := |J(k_1)/H| \leq \frac{(2g-1)!g^{2^{2g-1}}}{(1-\epsilon_q)^{2^{2g-1}}}.$$

*Proof.* We have

$$\#H = \frac{q^g(1 + \Delta_q)}{I}.$$

Observe that

$$\#(C(k_1) \setminus D)^{2g-1} = \frac{1}{(2g-1)!} q^{2g-1} (1 + \delta_q)^{2g-1} (1 - \epsilon_1)^{2g-1}.$$

On the other hand,  $C^{(2g-1)} \rightarrow J^1$  is a split projective bundle of relative dimension  $g-1$ . This implies that

$$\frac{1}{(2g-1)!} q^{2g-1} (1 + \delta_q)^{2g-1} (1 - \epsilon_q)^{2g-1} \leq \frac{q^g(1 + \Delta_q)}{I} \cdot \frac{q^g - 1}{q - 1}.$$

Using the bound (11), we obtain

$$I < \frac{(2g-1)!g}{((1 + \delta_q)(1 - \epsilon_q))^{2g-1}}.$$

□

Recall that the Galois group  $\Gamma := \text{Gal}(k/k_0)$  is isomorphic to  $\hat{\mathbb{Z}} = \prod_{\ell} \mathbb{Z}_{\ell}$  and is topologically generated by the Frobenius automorphism  $\text{Fr}$ . For a finite set of primes  $S$  let  $k_S \subset k$  be the fixed field of  $\Gamma_S := \prod_{\ell \notin S} \mathbb{Z}_{\ell}$ ; the Galois group of the (infinite) extension  $k_S/k_0$  is  $\prod_{\ell \in S} \mathbb{Z}_{\ell}$ . Note that  $J\{S\} \subset J(k_S)$  and that  $C(k_S) \subset J(k_S)$  is infinite. We have a natural projection map

$$\lambda_S : C(k) \rightarrow J(k) \rightarrow J\{S\},$$

(depending on the choice of  $c_0$ ).

**Theorem 5.6.** *Let  $S$  be a finite set of primes. Then*

- *the set  $C(k) \cap J\{S\}$  is finite;*
- *the map  $\lambda_S : C(k_S) \rightarrow J\{S\}$  is surjective with infinite fibers.*

*Proof.* The first statement is due to Boxall [Box92]. The second was proved in [BT05a]. □

**Remark 5.7.** Boxall's theorem can be proved using the following statement. Let  $\Gamma \simeq \mathbb{Z}_{\ell} \subset \text{GL}_n(\mathbb{Z}_{\ell})$  be an analytic semi-simple subgroup such that for all  $F \in \Gamma$  one has  $F - 1 \in \text{GL}_n(\mathbb{Q}_{\ell})$ . Consider the induced action of  $\Gamma$  on the torsion group  $(\mathbb{Q}_{\ell}/\mathbb{Z}_{\ell})^n$ . Then for all  $m \in \mathbb{N}$  there is an  $r \in \mathbb{N}$  such that for all  $x$  with  $\text{ord}(x) > \ell^r$  the orbit of  $x$  contains a translation of  $x$  by a cyclic subgroup of order  $> \ell^n$ .

**Remark 5.8.** Theorem 5.6 admits a generalization: Let  $X \subset A$  be a proper subvariety of an abelian variety. If  $S$  is a finite set of primes and if the intersection  $Y := X(k) \cap \prod_{\ell \in S} A\{\ell\}$  is infinite then

$$Y \subset (\cup_{i \in I} x_i + A_i(k)) \subset X(k) \subset A(k),$$

where  $I$  is a finite set,  $A_i \subset A$  are abelian subvarieties and  $x_i \in A(k)$  [Box92].

Note that for finite fields  $k_0$  with  $\#k_0$  sufficiently large, the image of  $C(k_0)^{(\mathbf{g})}$  does not coincide with  $J(k_0)$ . Indeed, the number of  $\mathbb{F}_q$ -points in  $C(\mathbb{F}_q)^{(\mathbf{g})}$  is approximately equal to

$$\frac{q^{\mathbf{g}}}{\mathbf{g}!} < q^{\mathbf{g}}.$$

On the other hand, among infinite extensions of  $k'/k_0$  we can easily find some with  $C(k')^{(g)} = J(k')$ .

**Proposition 5.9.** *Let  $k_0$  be a finite field with algebraic closure  $k$ ,  $S$  the set of primes  $\leq \mathbf{g}$  and  $\Gamma_S = \prod_{\ell \notin S} \mathbb{Z}_\ell \subset \text{Gal}(k/k_0)$ . Put  $k' := k^{\Gamma_S}$ . Then*

$$C(k')^{(\mathbf{g})} = J(k').$$

*Proof.* There exists a subvariety  $Y \subset J$  of codimension  $\geq 2$  such that for all  $x \in J(k) \setminus Y(k)$  there is a unique representation  $x = \sum_{i=1}^{\mathbf{g}} c_i$ , with  $c_i \in C(k)$ , modulo permutations.

Assume that  $x \in J(k') \setminus Y(k')$  and that its representation as a cycle contains at least one  $c_i \notin C(k')$ . For any  $\gamma \in \Gamma_S$  we have  $x = \sum_{i=1}^{\mathbf{g}} \gamma(c_i)$ . If  $\gamma \neq 1$ , then the size of any nontrivial orbit of  $\gamma$  is strictly greater than  $\mathbf{g}$ . Thus there is more than one representation of  $x$  as a sum of points in  $C(k)$ , modulo permutations within the cycle. Contradiction.

Assume that  $x \in Y(k')$ . Consider the fibration  $C^{(g)} \rightarrow J$ . The fiber over  $x$  is the projective space  $\mathbb{P}^r$ , defined over  $k'$ , parametrizing all representations of  $x$  as a sum of degree  $\mathbf{g}$  zero-cycles. There exists  $(c_1, \dots, c_{\mathbf{g}}) \in C^{(g)}(k')$  with  $\sum_{i=1}^{\mathbf{g}} c_i = x$ . We are done if  $c_i \in C(k')$ , for all  $i$ . Otherwise, we can apply the argument above, observing that  $\Gamma_S$  preserves this cycle.  $\square$

**Lemma 5.10.** Let  $J_\gamma(k) \subset J(k)$  be the subgroup of elements fixed by  $\gamma \in G_C$ . If  $C$  is not hyperelliptic then

$$j_\gamma : C(k) \setminus C_\gamma(k) \rightarrow J(k)/J_\gamma(k)$$

is an embedding of sets. If  $C$  is hyperelliptic let

$$C[4] := \{c \in C(k) \mid c \in J[4] \text{ and } \gamma(c) = -c\}.$$

Then

$$j_\gamma : C(k) \setminus (C_\gamma(k) \cup C[4]) \rightarrow J(k)/J_\gamma(k)$$

is an embedding of sets.

*Proof.* Assume there exist two points  $c, c' \in C(k)$  with  $\gamma(c) \neq c$  and  $\gamma(c') \neq c'$  and such that  $j_\gamma(c) = j_\gamma(c')$ . Then  $\gamma(c) - \gamma(c') = c - c'$  and hence  $\gamma(c) + c' = c + \gamma(c')$ . The cycles  $\gamma(c) + c', c + \gamma(c')$  consist of different points since  $c' \neq c, c' \neq \gamma(c')$ , by assumption. Thus  $\gamma(c) + c'$  defines a hyperelliptic pencil and we have proved the lemma for nonhyperelliptic curves.

In the hyperelliptic case assume that the pencil consists of elements  $c, -c$  (since the pencil is clearly  $\gamma$ -invariant and belongs to  $J_\gamma$ ). Thus  $c' = -c$  and  $\gamma$  acts as  $-1$  on  $c$ . Note that  $j_\gamma(c) = -j_\gamma(c)$  implies that  $j_\gamma(2c) = 0$  and  $2c \in J_\gamma(k)$ . Then  $2c = -2c$  implies that  $4c = 0$ . Thus in this case a possible exceptional subset consists of points  $c \neq c' = -c$  of order 4 such that  $\gamma(c) = -c$ .  $\square$

**Theorem 5.11.** *The group of automorphisms  $G_C$  satisfies conditions of Proposition 4.5.*

*Proof.* By Lemma 3.2, there is an injective continuous homomorphism

$$\psi = \psi_\ell : G_C \rightarrow \prod_{\ell} \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

Moreover, for all nontrivial  $\gamma \in G_C$  the image  $\psi_\ell(\gamma) \neq 1$ , for infinitely many  $\ell$ . Otherwise, let  $S$  be the finite set of primes such that  $\psi_\ell(\gamma)$  is trivial for  $\ell \notin S$ . Then

- $J\{S\} \rightarrow J(k)/J_\gamma(k)$  is a surjection;
- $C(k) \rightarrow J(k)/J_\gamma(k)$  is finite outside  $0 \in J(k)/J_\gamma(k)$ , by Lemma 5.10;
- $C(k) \rightarrow J\{S\}$  is a surjection with infinite fibers over every point, by Theorem 5.6.

Contradiction.  $\square$

**Corollary 5.12.** *For all  $\gamma, \tilde{\gamma} \in G_C$  there exists an  $n \in \mathbb{N}$  such that  $\gamma^n$  and  $\tilde{\gamma}^n$  commute.*

*Proof.* It suffices to combine Theorem 5.11 and Proposition 4.5.  $\square$

**Theorem 5.13.** *Let  $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$  be an isomorphism of pairs. Then there exists an  $n \in \mathbb{N}$  such that  $\mathrm{Fr}_C^n$  and  $\phi^{-1}(\mathrm{Fr}_{\tilde{C}}^n)$  commute in  $\mathrm{End}_k(J)$ .*

*Proof.* Immediate from Theorem 5.11 and Corollary 5.12.  $\square$

**Lemma 5.14.** Assume that  $\mathrm{Fr}$  and  $\tilde{\mathrm{Fr}}$  generate the same  $\ell$ -adic subgroup in  $\mathrm{GL}_n(\mathbb{Z}_\ell)$ . Then there exist  $n, \tilde{n} \in \mathbb{N}$  such that

$$\mathrm{Fr}^n = \tilde{\mathrm{Fr}}^{\tilde{n}}.$$

*Proof.* The assumption implies that there exist an  $\alpha \in \mathbb{Z}_\ell^*$  and an  $\tilde{n} \in \mathbb{N}$  such that

$$\mathrm{Fr}^\alpha = \tilde{\mathrm{Fr}}^{\tilde{n}}.$$

The same equality holds for the determinants. However, the determinants are positive integer powers of  $p$ .  $\square$

## 6. Detecting isogenies

In this section, we recall some facts from divisibility theory for linear recurrences, as developed in [CZ02], and apply these to derive a sufficient condition for isogeny of abelian varieties.

A function  $F : \mathbb{N} \rightarrow \mathbb{C}$  is called a *linear recurrence* if there exist an  $r \in \mathbb{N}$ , and  $a_i \in \mathbb{C}$ , such that for all  $n \in \mathbb{N}$  one has

$$F(n+r) = \sum_{i=0}^{r-1} a_i F(n+i).$$

There is a unique expression

$$F(n) = \sum_{i=1}^m f_i(n) \gamma_i^n,$$

where  $f_i \in \mathbb{C}[x]$  are nonzero and  $\gamma_i \in \mathbb{C}^*$ . The complex numbers  $\gamma_i \in \mathbb{C}^*$  are called the roots of the recurrence. Let  $\Gamma$  be a torsion-free finitely-generated subgroup of the multiplicative group  $\mathbb{C}^*$ . Then the ring of linear recurrences with roots in  $\Gamma$  is isomorphic to the unique factorization domain  $\mathbb{C}[x, \Gamma]$  (see [CZ02, Lemma 2.1]); the element in  $\mathbb{C}[x, \Gamma]$  corresponding to a linear recurrence  $F$  will be denoted by the same letter.

We say that  $\{F(n)\}_{n \in \mathbb{N}}$  is a *simple* linear recurrence, if  $\deg(f_i) = 0$ , for all  $i$ , i.e.,  $f_i$  are constants.

**Proposition 6.1.** *Let  $\{F(n)\}_{n \in \mathbb{N}}, \{\tilde{F}(n)\}_{n \in \mathbb{N}}$  be simple linear recurrences such that  $F(n), \tilde{F}(\tilde{n}) \neq 0$  for all  $n, \tilde{n} \in \mathbb{N}$ . Assume that*

1. *The set of roots of  $F$  and  $\tilde{F}$  generates a torsion-free subgroup of  $\mathbb{C}^*$ .*
2. *There is a finitely-generated subring  $\mathfrak{R} \subset \mathbb{C}$  with  $F(n)/\tilde{F}(\tilde{n}) \in \mathfrak{R}$ , for infinitely many  $n \in \mathbb{N}$ .*

*Then*

$$\begin{aligned} G : \mathbb{N} &\rightarrow \mathbb{C} \\ n &\mapsto F(n)/\tilde{F}(\tilde{n}) \end{aligned}$$

*is a simple linear recurrence.*

*Proof.* The fact that  $G$  is a linear recurrence is proved in [CZ02, p. 434]. Enlarging  $\Gamma$ , if necessary, we obtain an identity

$$G \cdot \tilde{F} = F,$$

in the ring  $\mathbb{C}[x, \Gamma]$ . Since  $F, \tilde{F}$  are simple, i.e., in  $\mathbb{C}[\Gamma]$ ,  $G$  is also simple. □



**Lemma 6.2.** Let  $\Gamma$  be a finitely-generated torsion-free abelian group of rank  $r$  with a fixed basis  $\{\gamma_1, \dots, \gamma_r\}$ . Let  $\mathbb{C}[\Gamma]$  be the corresponding algebra of Laurent polynomials, i.e., finite linear combinations of monomials  $x^\gamma = \prod_{j=1}^r x_j^{g_j}$ , where  $\gamma = \sum_{i=1}^r g_i \gamma_i \in \Gamma$ . Let  $\gamma$  be a primitive element in  $\Gamma$ , i.e.,  $\gcd(g_1, \dots, g_r) = 1$ . Then, for each  $\lambda \in \mathbb{C}^*$ , the polynomial  $x^\gamma - \lambda$  is irreducible in  $\mathbb{C}[\Gamma]$ , i.e., defines an irreducible hypersurface in the torus  $(\mathbb{C}^*)^r$ .

Let  $\gamma, \gamma' \in \Gamma$  be arbitrary elements. The polynomials  $x^\gamma - 1$  and  $x^{\gamma'} - 1$  are not coprime in  $\mathbb{C}[\Gamma]$ , i.e., the corresponding divisors in  $(\mathbb{C}^*)^r$  have common irreducible components, if and only if  $\gamma, \gamma'$  generate a cyclic subgroup of  $\Gamma$ .

*Proof.* The map defined by the monomial  $x^\gamma : (\mathbb{C}^*)^r \rightarrow \mathbb{C}^*$  has irreducible fibers, if and only if  $\gamma$  is primitive. For other  $\gamma$ , put  $m := \gcd(g_1, \dots, g_r) > 1$  and  $\gamma = m\tilde{\gamma}$ . Then  $x^\gamma - 1 = \prod_{s=1}^m (x^{\tilde{\gamma}} - \zeta_m^s)$ , where  $\zeta_m$  is a primitive  $m$ -th root of 1. By the first observation, the polynomials  $x^{\tilde{\gamma}} - \zeta_m^s$  are irreducible. To prove the last statement, note that coprimality of  $x^\gamma - 1$  and  $x^{\gamma'} - 1$  is equivalent to coprimality of  $x^{\tilde{\gamma}} - 1$  and  $x^{\tilde{\gamma}'} - 1$ , for the corresponding primitivizations  $\tilde{\gamma}, \tilde{\gamma}'$  of  $\gamma, \gamma'$ . This coprimality is equivalent to  $\tilde{\gamma} \neq \pm \tilde{\gamma}'$ .  $\square$

Let  $A$  be an abelian variety of dimension  $g$  defined over a finite field  $k_1$  of characteristic  $p$ , and let  $\{\alpha_j\}_{j=1, \dots, 2g}$  be the set of eigenvalues of the corresponding Frobenius endomorphism  $\text{Fr}$  on the  $\ell$ -adic cohomology, for  $\ell \neq p$ . Let  $k_n/k_1$  be the unique extension of degree  $n$ . The sequence

$$F(n) := \#A(k_n) = \prod_{j=1}^{2g} (\alpha_j^n - 1). \quad (12)$$

is a simple linear recurrence. Let  $\Gamma$  be the multiplicative subgroup of  $\mathbb{C}^*$  generated by  $\{\alpha_j\}_{j=1, \dots, 2g}$ . Choosing  $k_1$  sufficiently large, we may assume that  $\Gamma$  is torsion-free. Choose a basis  $\gamma_1, \dots, \gamma_r$  of  $\Gamma$ , and write

$$\alpha_j = \prod_{i=1}^r \gamma_i^{a_{ij}},$$

with  $a_{ij} \in \mathbb{Z}$ . Recall that all  $\alpha_j$  are Weil numbers, i.e., all Galois-conjugates of  $\alpha_j$  have absolute value  $\sqrt{q}$ , where  $q = \#k_1$ . It follows that, for  $j \neq j'$ , either  $\alpha_j = \alpha_{j'}$  or  $\alpha_j, \alpha_{j'}$  generate a subgroup of rank two in  $\Gamma$  (since  $\Gamma$  does not contain torsion elements). We get a subdivision of the sequence of eigenvalues

$$\{\alpha_j\}_{j=1, \dots, 2g} = \sqcup_{s=1}^t I_s, \quad t \leq 2g,$$

into subsets of equal elements. Put  $d_s = \#I_s$  and let  $\alpha_s \in I_s$ .

**Theorem 6.3.** Let  $A$  and  $\tilde{A}$  be abelian varieties of dimension  $g$  over finite fields  $k_1$ , resp.  $\tilde{k}_1$ . Let  $F$ , resp.  $\tilde{F}$ , be a simple linear recurrence as in equation (12). Assume that  $F(n) \mid \tilde{F}(n)$  for infinitely many  $n \in \mathbb{N}$ . Then  $A$  and  $\tilde{A}$  are isogenous.

*Proof.* Let  $\Gamma \in \mathbb{C}^*$  be the (multiplicative) subgroup generated by  $\{\alpha_j\} \cup \{\tilde{\alpha}_j\}$ . Enlarging  $k_1$ , resp.  $\tilde{k}_1$ , we may assume that  $\Gamma$  is torsion-free. Proposition 6.1 implies that  $F/\tilde{F}$  is a simple linear recurrence.

The Laurent polynomial corresponding to  $F$ , resp.  $\tilde{F}$ , has the form

$$\prod_{s=1}^t \left( \prod_{i=1}^r x_i^{a_{is}} - 1 \right)^{d_s}, \quad \text{resp.} \quad \prod_{\tilde{s}=1}^{\tilde{t}} \left( \prod_{i=1}^r x_i^{\tilde{a}_{i\tilde{s}}} - 1 \right)^{d_{\tilde{s}}}.$$

Observe, that

$$\gcd\left(\prod_{i=1}^r x_i^{a_{is}} - 1, \prod_{i=1}^r x_i^{a_{is'}} - 1\right) \in \mathbb{C}^*,$$

for  $s \neq s'$ . The same holds for  $\tilde{F}$ . Using Lemma 6.2, we conclude that  $t = \tilde{t}$ , that we can order the indices so that  $\#I_s = \#\tilde{I}_s$ , and so that the multiplicative groups generated by  $\alpha_s \in I_s$  and  $\tilde{\alpha}_s \in \tilde{I}_s$  have rank 1, for each  $s = 1, \dots, t$ . Thus  $\tilde{\alpha}_s = \alpha_s^u$ , where  $u \in \mathbb{Q}$  depends only on  $k_1$  and  $\tilde{k}_1$ . It follows that some integer powers of  $\text{Fr}, \tilde{\text{Fr}}$  have the same sets of eigenvalues, with equal multiplicities. It suffices to apply Theorem 1.1 to conclude that  $A$  is isogenous to  $\tilde{A}$ .  $\square$

## 7. Reconstruction

We return to the setup in Section 1:  $C, \tilde{C}$  are irreducible smooth projective curves over  $k$  of genus  $\geq 2$ , with Jacobians  $J$ , resp.  $\tilde{J}$ . We have a diagram

$$\begin{array}{ccccc} J(k) & & J^1(k) & \xleftarrow{j_1} & C(k) \\ \phi^0 \downarrow & & \phi^1 \downarrow & & \phi_s \downarrow \\ \tilde{J}(k) & & \tilde{J}^1(k) & \xleftarrow{\tilde{j}_1} & \tilde{C}(k) \end{array}$$

where

- $\phi^0$  is an isomorphism of abstract abelian groups;
- $\phi^1$  is an isomorphism of homogeneous spaces, compatible with  $\phi^0$ ;
- the restriction  $\phi_s : C(k) \rightarrow \tilde{C}(k)$  of  $\phi^1$  is a bijection of sets.

It will be convenient to choose a point  $c_0 \in C(k_0)$  and fix the embeddings

$$\begin{array}{ccc} C(k) & \rightarrow & J(k) \\ c & \mapsto & c - c_0 \end{array} \quad \begin{array}{ccc} \tilde{C}(k) & \rightarrow & \tilde{J}(k) \\ \tilde{c} & \mapsto & \tilde{c} - \phi_s(c_0). \end{array}$$

With this choice, the isomorphism of abelian groups  $\phi$  induces a bijection on the sets  $C(k)$  and  $\tilde{C}(k)$ . In this situation we will say that

$$\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$$

is an isomorphism of pairs.

**Lemma 7.1.** For any choice of  $n_1, \dots, n_r \in \mathbb{N}$  and  $c_1, \dots, c_r \in C(k)$  one has

$$\dim H^0(C, \mathcal{O}(\sum_i n_i c_i)) = \dim H^0(\tilde{C}, \mathcal{O}(\sum_i n_i \phi^0(c_i))).$$

*Proof.* The effectivity of a divisor on  $C$  is intrinsically determined by the group  $J(k)$ : the images of the maps  $C^{(d)} \rightarrow J$ , resp.  $\tilde{C}^{(d)} \rightarrow \tilde{J}$ , are the same (under  $\phi^0$ ). We can distinguish  $D \in J(k)$  with  $\dim H^0(C, D) \geq 1$ , and therefore all sets of linearly equivalent divisors. By induction, we can detect that  $\dim H^0(C, D) \geq n$ , with  $n > 1$ : there are infinitely many points  $c \in C(k) \subset J(k)$  such that  $\dim H^0(C, D - c) \geq n - 1$ .  $\square$

**Corollary 7.2.** *If  $C$  is hyperelliptic, trigonal or special (i.e., violate the Brill–Noether inequality) then so is  $\tilde{C}$ .*

**Corollary 7.3.** *Let  $A \subset C^{(d)} \hookrightarrow J$ , for  $d < g$ , be a proper abelian subvariety. Then there is a proper abelian subvariety  $\tilde{A} \subset \tilde{C}^{(d)} \hookrightarrow \tilde{J}$  such that  $\phi^0$  induces an isomorphism between  $A$  and  $\tilde{A}$ .*

*Proof.* Any such abelian subvariety of maximal dimension is characterized by the property that it contains an arbitrarily large abelian subgroup of rank equal to twice its dimension. In particular,  $\phi^0$  induces an isomorphism on such subvarieties.  $\square$

**Lemma 7.4.** Assume that  $g(C) > 2$  and that  $C$  is bielliptic. Then  $\tilde{C}$  is also bielliptic and the map  $\phi^0$  commutes with every bielliptic involution on  $C$  and  $\tilde{C}$ , respectively.

Recall that a bielliptic structure is a map  $j_E : C \rightarrow E$  of degree 2, where  $E$  is an elliptic curve. By Theorem 10.3, all bielliptic structures correspond to embedded elliptic curves  $E \subset C^{(2)} \subset J$ . Since we assume  $g(C) > 2$ , there is a finite number of such embeddings and they are preserved under  $\phi^0$ . Thus if  $C$  is bielliptic then so is  $\tilde{C}$ , and the groups generated by bielliptic reflections are isomorphic.

**Corollary 7.5.** *If  $C$  is the Klein curve then  $\tilde{C}$  is also a Klein curve. Indeed, this is a unique curve of genus 3 which has the action of  $\mathrm{PGL}_2(\mathbb{F}_7)$ . The action is generated by bielliptic involutions and hence  $\tilde{C}$  is isomorphic to  $C$ .*

**Remark 7.6.** Note that the isomorphism  $\phi^0$  itself does not have to be algebraic, a profinite power of the Frobenius will have the same properties.

Assume that  $\mathrm{char}(k_0) \neq 2$ , and that  $\#k_0$  is sufficiently large, i.e., for all finite extensions  $k_1/k_0$  the points  $C(k_1)$  generate  $J(k_1)$ , and same for  $\tilde{C}$ .

**Lemma 7.7.** Assume that  $C$  and  $\tilde{C}$  are not hyperelliptic. Fix finite fields  $k_0, \tilde{k}_0$  such that  $\#k_0, \#\tilde{k}_0$  are sufficiently large and  $J(k_0) \subset \tilde{J}(\tilde{k}_0)$ . Consider the tower of field extensions:  $k_0 \subset k_1 \subset \dots$ , where  $k_i/k_{i-1}$  is the unique extension of degree 2, and similarly for  $\tilde{k}_0$ . Then, for all  $n \in \mathbb{N}$ ,

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n).$$

*Proof.* We have an intrinsic inductive characterization of  $C(k_n)$  and  $J(k_n)$ , resp.  $\tilde{C}(\tilde{k}_n)$  and  $\tilde{J}(\tilde{k}_n)$ . Namely,  $c \in C(k_n) \setminus C(k_{n-1})$ , iff there exists a point  $c' \in C(k)$  such that  $c + c' \in J(k_{n-1})$ . Indeed, if  $c \in C(k_n)$  then  $c'$  is the conjugate for the Galois automorphism  $\sigma$  of  $k_n/k_{n-1}$ . Conversely, if  $c + c'$  is a pair as above and  $\sigma(c) \neq c'$ , then  $\sigma(c + c') = c + c' \in J(k)$ , which defines a nontrivial hyperelliptic pencil on  $C$ , contradicting our assumption. By assumption on  $k_0$ , points  $C(k_n)$  generate  $J(k_n)$ , as an abelian group. By induction, it follows that  $\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n)$ .  $\square$

By Corollary 7.2, the hyperelliptic property of  $C$  implies the same for  $\tilde{C}$ . The hyperelliptic case requires a more delicate analysis of point configurations.

Let  $C$  be a hyperelliptic curve over a finite field  $\mathbb{F}_q$ . The Jacobian  $J^2$  of zero cycles of degree 2 contains a unique effective zero-cycle  $z_0 \in J^2(\mathbb{F}_q)$  corresponding to the hyperelliptic pencil on  $C$ . We use this cycle to identify  $J^2(k) \simeq J(k) = J^0(k)$ . Let  $k_0/\mathbb{F}_q$  be a finite extension,  $k_1/k_0$  a quadratic extension and  $\sigma$  the nontrivial element of the Galois group  $\text{Gal}(k_1/k_0)$ . Put

$$C(k_1)^- := \{c \in C(k_1) \mid \sigma(c) + c = z_0 \in J^2(k_0)\}.$$

**Lemma 7.8.** Let  $C$  be a hyperelliptic curve defined over  $\mathbb{F}_q$ . Then there exists an  $N \in \mathbb{N}$  such that for all finite extensions  $k_0/\mathbb{F}_q$  with  $q^N \mid \#k_0$ , the zero-cycles of even degree with support in  $C(k_1) \setminus C(k_1)^-$  generate  $J(k_1) \simeq J^2(k_1)$ .

*Proof.* Let  $H \subset J(k_1)$  be the subgroup generated by zero-cycles of even degree with support in  $C(k_1) \setminus C(k_1)^-$ . Put  $q := \#k_0$ . Note that

$$|\#C(k_1)^- - q| \leq 2g\sqrt{q}.$$

Indeed, let  $\iota : C \rightarrow \mathbb{P}^1$  be the hyperelliptic projection. Then  $\iota(C(k_1)^-) \subseteq \mathbb{P}^1(k_0)$ , and the image corresponds to those points on  $b \in \mathbb{P}^1(k_0)$  such that the degree 2 cycle  $\iota^{-1}(b)$  does not split over  $k_0$ . The claim follows from standard Weil estimates. Lemma 5.5 implies a universal ( $k_1$  independent) bound for the index  $I := [J(k_1) : H]$ , e.g.,  $I < m$ .

Now we apply the argument of Lemma 5.2. Let  $k_0$  be such that  $J(k_0)$  contains all  $J(k)[\ell]$ , for  $\ell < m$ . Then  $H = J(k_1)$ . Indeed, for  $\ell \neq 2$  and  $J(k)[\ell] \subset J(k_0)$  the order of  $J(k_1)/J(k_0)$  is coprime to  $\ell$ : if an automorphism of order 2 acts trivially on  $J(k)[\ell]$  then it also acts trivially on all elements of  $\ell$ -power order in  $J(k_1)$ . Next, note that the elements of the form  $\frac{1}{2}x, x \in J(k_0)$  generate the 2-primary part of  $J(k_1)$  but that  $\sigma(\frac{1}{2}x) = x + z_0, z_0 \in J^2(k_0)$  and hence  $\frac{1}{2}x$  is never in  $J(k_1)^-$  (the subgroup generated by  $C(k_1)^-$ ). This completes the argument for  $\ell = 2$ .  $\square$

**Lemma 7.9.** Assume that  $C$  and  $\tilde{C}$  are hyperelliptic. There exist finite fields  $k_0, \tilde{k}_0$  and towers of quadratic field extensions:  $k_0 \subset k_1 \subset \dots$ , resp. for  $\tilde{k}_0$ , such that for all  $n \in \mathbb{N}$

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n).$$

*Proof.* By Lemma 7.8, the points in  $C(k_i) \setminus C(k_i)^-$  generate  $J(k_i)$ . This subset of points is defined intrinsically in  $C(k)$ , provided  $J(k_{i-1})$  is already known. By induction, as in the proof of Lemma 7.7, we obtain the required tower of degree 2 extensions, with an embedding

$$\phi^0 : J(k_i) \rightarrow \tilde{J}(\tilde{k}_i).$$

□

**Theorem 7.10.** *Let  $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$  be an isomorphism of pairs. Then  $J$  and  $\tilde{J}$  are isogenous.*

*Proof.* In both hyperelliptic and nonhyperelliptic case we have shown that, for sufficiently large finite ground fields  $k_0, \tilde{k}_0$ , there exist towers  $\{k_n\}_{n \in \mathbb{N}}$  and  $\{\tilde{k}_n\}_{n \in \mathbb{N}}$  of degree 2 field extensions with the following property:

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n)$$

(see Lemma 7.7 and Lemma 7.9). Now we apply Theorem 6.3 to the Frobenius automorphisms  $\text{Fr}, \tilde{\text{Fr}}$ . □

## 8. Generalized Jacobians

Let  $k$  be a field and  $K/k$  a field extension. Then the set

$$\mathbb{P}(K) := K^*/k^* = (K \setminus 0)/k^*$$

carries the structure of an abelian group *and* a projective space. Moreover, the projective structure (the set of projective lines, their intersections etc.) is compatible with the group operation. We have:

**Theorem 8.1.** *Let  $K$  and  $\tilde{K}$  be function fields over  $k$ . Assume that we have an isomorphism of abelian groups*

$$\phi_{gr} : K^*/k^* \rightarrow \tilde{K}^*/k^*$$

*inducing an isomorphism of projective structures*

$$\phi_{pr} : \mathbb{P}(K) \rightarrow \mathbb{P}(\tilde{K}).$$

*Then there exists an isomorphism of fields*

$$\phi_f : K \rightarrow \tilde{K}.$$

*Proof.* See [BT04], Section 4, for precise definitions and a proof. □

We will apply this Theorem to  $K = k(C)$  and  $\tilde{K} = k(\tilde{C})$ .

We write  $J = J$  and  $J^1 = J^1$ , resp.  $\tilde{J}$  and  $\tilde{J}^1$ , for the Jacobian of degree 0 and degree 1 zero-cycles on  $C$ , resp.  $\tilde{C}$ . Let  $Z^0(k) = Z^0(C(k))$ , resp.  $\tilde{Z}^0(k)$ , be the group of degree 0 zero-cycles on  $C$ , resp.  $\tilde{C}$ . We have a diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & K^*/k^* & \longrightarrow & Z^0(k) & \longrightarrow & J(k) \longrightarrow 1 \\ & & & & \downarrow \phi^0 & & \downarrow \phi \\ 1 & \longrightarrow & \tilde{K}/k^* & \longrightarrow & \tilde{Z}^0(k) & \longrightarrow & \tilde{J}^0(k) \longrightarrow 1 \end{array}$$

where  $\phi_0$  is an isomorphism of abelian groups induced by  $\phi$  and  $\phi_s$ . This implies the following

**Lemma 8.2.** Under the assumptions of Conjecture 1.3, we have an isomorphism of abelian groups

$$\phi_{gr} : K^*/k^* \rightarrow \tilde{K}^*/k^*.$$

We have a natural embedding  $C \hookrightarrow J^1$  from (1), mapping a point in  $C(k)$  to its cycle-class. Choosing a point  $c_0 \in C(k)$  we also have an embedding

$$\begin{array}{ccc} C(k) & \hookrightarrow & J(k) \\ c & \mapsto & [c - c_0] \end{array} \quad (13)$$

Write  $\mathfrak{m} = \sum_{i=1}^r n_i P_i$ ,  $n_i \in \mathbb{Z} \setminus 0$ ,  $P_i \in C(k)$  for a zero-cycle on  $C$  and  $|\mathfrak{m}| := P_1 \cup \dots \cup P_r$  for its support. Let  $Z_{\mathfrak{m}}^0(k) = Z_{\mathfrak{m}}^0(C(k))$  be the group of degree 0 zero-cycles with support disjoint from the support of  $\mathfrak{m}$ .

For every effective  $k$ -rational zero-cycle  $\mathfrak{m}$  let  $J_{\mathfrak{m}}(k)$ , resp.  $J_{\mathfrak{m}}^1$ , be the *generalized Jacobian* of degree 0, resp. degree 1, zero-cycles on  $C$  over  $k$ , modulo the ideal generated by  $\mathfrak{m}$ . The generalized Jacobian  $J_{\mathfrak{m}}$  is an algebraic group, fibered over the Jacobian  $J$  with fibers connected abelian linear algebraic groups of dimension  $\#\mathfrak{m} - 1$ .

We have a compatible family of embeddings

$$\mu_{\mathfrak{m}}^1 : C(k) \setminus |\mathfrak{m}| \hookrightarrow J_{\mathfrak{m}}^1(k) \quad (14)$$

as well as surjective homomorphisms of abelian groups

$$\mu_{\mathfrak{m}} : Z_{\mathfrak{m}}^0(k) \rightarrow J_{\mathfrak{m}}(k). \quad (15)$$

The natural embedding  $C \hookrightarrow J^1$ , assigning to a point  $c \in C(k)$  its cycle class  $[c] \in J(k)$  extends uniquely to a compatible family of maps

$$\mu_{\mathfrak{m}} : C \setminus |\mathfrak{m}| \hookrightarrow J_{\mathfrak{m}}^1.$$

**Proposition 8.3.** *Assume that for all  $\mathfrak{m} = P + R$  one has an isomorphism of abelian groups*

$$\phi_{\mathfrak{m}}^0 : J_{\mathfrak{m}}(k) \rightarrow \tilde{J}_{\mathfrak{m}}(k)$$

*and a diagram (of compatible maps)*

$$\begin{array}{ccccccc} C(k) \setminus |\mathfrak{m}| & \xrightarrow{\mu_{\mathfrak{m}}} & J_{\mathfrak{m}}^1(k) & \xrightarrow{\phi_{\mathfrak{m}}^1} & \tilde{J}_{\mathfrak{m}}^1(k) & \xleftarrow{\tilde{\mu}_{\mathfrak{m}}} & \tilde{C}(k) \setminus |\mathfrak{m}| \\ \downarrow & & \downarrow \varphi_{\mathfrak{m}} & & \downarrow \tilde{\varphi}_{\mathfrak{m}} & & \downarrow \\ C(k) & \longrightarrow & J^1(k) & \xrightarrow{\phi^1} & \tilde{J}^1(k) & \longleftarrow & \tilde{C}(k) \end{array}$$

*with  $\phi^1, \phi_{\mathfrak{m}}^1$  isomorphisms of homogeneous spaces under  $J_{\mathfrak{m}}(k) \simeq \tilde{J}_{\mathfrak{m}}(k)$  inducing bijections of sets*

$$C(k) \setminus \mathfrak{m} = \tilde{C}(k) \setminus \mathfrak{m}$$

*Then  $k(C) = k(\tilde{C})$ .*

*Proof.* It suffices to prove that the isomorphism of groups

$$\phi_{gr} : K^*/k^* \rightarrow \tilde{K}^*/k^*$$

established in Lemma 8.2 preserves the respective projective structures. A projective line in  $\mathbb{P}(K)$  is the projectivization of a two-dimensional  $k$ -vector space generated by two functions  $f, g \in K^*$ . By the compatibility with multiplication in  $K^*/k^*$ , we can assume that  $g = 1$ .

Every pair of rationally equivalent effective zero-cycles  $z_0, z_{\infty}$  on  $C(k)$  defines a unique “point” in  $K^*/k^* = \mathbb{P}(K)$  - the divisor of a function  $f$  with zeroes  $z_0$  and poles  $z_{\infty}$ . To get a projective line  $\mathbb{P}^1 \subset \mathbb{P}(K)$  consider the map  $\pi_f : C \rightarrow \mathbb{P}^1$  defined by  $f$  and the induced family of cycles  $z_{\lambda} := \pi_f^{-1}(\lambda)$ , for  $\lambda \in \mathbb{P}^1$ . The family of “points” in  $\mathbb{P}(K)$ , given by cycles  $z_{\lambda} - z_{\infty}$ , is a projective line in  $\mathbb{P}(K)$  through 1 and  $f$ .

Conversely, assume that for every such pair  $z_0, z_{\infty}$  of equivalent effective cycles on  $C$  we have an intrinsic definition of the set  $z_{\lambda}$ . Then we recover the projective structure on  $\mathbb{P}(K)$ .

We define an equivalence relation on  $C(k)$ :

$$P \sim Q \Leftrightarrow (z_0 - z_{\infty}) \in \text{Ker}(\mu_{\mathfrak{m}}),$$

where  $\mathfrak{m} = P + Q$ . Observe that  $P \sim Q$  iff  $P, Q$  are both contained in the fiber of  $\pi_f$ . The set  $\{z_{\lambda}\}$  is intrinsically defined as the set of equivalence classes with respect to “ $\sim$ ”.  $\square$

The group  $Z^0(k)$  is the set of  $k$ -points of a countable union of algebraic varieties

$$Z^0(k) = \cup_{n \in \mathbb{N}} (C^{(n)} \times C^{(n)})^\circ(k),$$

each parametrizing pairs of effective zero-cycles of degree  $n$  of disjoint support. This induces a grading on the subset  $K^*/k^* \subset Z^0(k)$ .

**Lemma 8.4.** The multiplicative group  $K^*/k^*$  is generated by components of degree  $\leq g + 1$ .

*Proof.* Let  $z, z'$  be effective cycles on  $C$ , of disjoint support, of degree  $n > g + 1$ . The space of cycles equivalent to  $z - z'$  has (projective) dimension  $\geq 2$ . Then there exists an effective cycle  $z''$ , equivalent to  $z$  and  $z'$ , such that  $|z| \cap |z'| \neq \emptyset$  and  $|z'| \cap |z''| \neq \emptyset$ . (Choose a hyperplane section in  $\mathbb{P}(H^0(C, \mathcal{O}(z - z')))$  which contains points from the support of both  $z$  and  $z'$ . The intersection of  $C$  with this hyperplane gives  $z''$ .) Now we can write

$$z - z' = (z - z'') + (z' - z'')$$

with  $(z - z'')$  and  $(z' - z'')$  having degree  $< n$ .  $\square$

Let  $Y^{\mathbf{g}+1}$ , resp.  $Y_{\mathbf{m}}^{\mathbf{g}+1}$ , be the subvariety of  $C^{(\mathbf{g}+1)} \times C^{(\mathbf{g}+1)}$  corresponding to pairs of effective degree  $\mathbf{g} + 1$  cycles of disjoint support, resp. in addition with support disjoint from  $|\mathbf{m}|$ . Each such pair of cycles  $(z_0, z_\infty)$  determines a principal divisor on  $C$ , thus a function  $f$ , modulo  $k^*$ , and an algebraic morphism  $Y_{\mathbf{m}}^{\mathbf{g}+1} \rightarrow \mathbb{G}_m$  which on the level of points is given by

$$\begin{aligned} Y_{\mathbf{m}}^{\mathbf{g}+1}(k) &\rightarrow k^* \\ (z_0, z_\infty) &\mapsto f(P)/f(Q). \end{aligned}$$

The algebraic variety  $X$ , resp.  $X_{\mathbf{m}}$  is defined as the preimage of  $1 \in \mathbb{G}_m$ . We get the diagram, with maps morphisms of algebraic varieties:

$$\begin{array}{ccccccc} 1 & \longrightarrow & X_{\mathbf{m}} & \longrightarrow & Y_{\mathbf{m}}^{\mathbf{g}+1} & \longrightarrow & J_{\mathbf{m}} \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & X & \longrightarrow & Y^{\mathbf{g}+1} & \longrightarrow & J \longrightarrow 1 \end{array}$$

and a similar diagram for  $\tilde{C}$ .

**Lemma 8.5.** Under the assumptions of Conjecture 1.3, we have a bijection of sets:

- $\phi_s^X : X(k) \rightarrow \tilde{X}(k)$
- $\phi_{s,\mathbf{m}}^X : X_{\mathbf{m}}(k) \rightarrow \tilde{X}_{\mathbf{m}}(k)$ .

*Proof.* It suffices to give the following intrinsic description:

$$Y_{\mathbf{m}}^{\mathbf{g}+1}(k) := \{(z_0, z_\infty) \mid P, Q \notin |z_0| \cup |z_\infty| \text{ and } P + Q \in |z_\lambda|, \text{ for some } \lambda\}$$

and a similarly for  $Y^{\mathbf{g}+1}(k)$ .  $\square$



## 9. Anabelian geometry

In this section we discuss an application of the above results to Grothendieck's Anabelian Program - the reconstruction of function fields from Galois groups.

Let  $C$  be an irreducible smooth projective curve over  $k = \bar{\mathbb{F}}_p$  of genus  $g \geq 2$ ,  $J$  its Jacobian and  $K = k(C)$  its function field. Throughout, we assume that  $p > 2$ . Fix an algebraic closure  $\bar{K}/K$  and let  $\mathcal{G} = \mathcal{G}_K = \text{Gal}(\bar{K}/K)$  be the absolute Galois group. The main idea of anabelian geometry is that  $\mathcal{G}$ , or even one of its factors, determines  $C$ . Note that  $\mathcal{G}$  is the completion of a free group with an infinite number of generators. In particular, for any two curves over  $k$  the corresponding groups are isomorphic as abstract topological groups. However, we will see that in some instances additional structures allow us to recover the curve from the Galois group.

Let

$$\mathcal{G}^a = \mathcal{G}/[\mathcal{G}, \mathcal{G}]$$

be the abelianization of  $\mathcal{G}$ . Let  $\ell$  be a prime number,  $\mathcal{G}_\ell$  the  $\ell$ -completion of  $\mathcal{G}$ , and  $\mathcal{G}_\ell^a$  the image of  $\mathcal{G}_\ell$  in the abelianization. Clearly,  $\mathcal{G}^a = \prod_\ell \mathcal{G}_\ell^a$ . A  $k$ -rational point  $c \in C(k)$  determines a discrete rank one valuation  $\nu = \nu_c$  of the function field  $K$ . We write  $\mathcal{I}_\nu \subset \mathcal{G}$  for the corresponding inertia subgroup and  $\mathcal{I}_\nu^a$ , resp.  $\mathcal{I}_{\nu, \ell}^a$ , for its image in  $\mathcal{G}^a$ , resp.  $\mathcal{G}_\ell^a$ . The group  $\mathcal{I}_\nu^a$  is topologically cyclic.

We now proceed to describe the groups  $\mathcal{G}_\ell^a$ , for  $\ell \neq p$  (the structure of  $\mathcal{G}_p^a$  is more refined), closely following Sections 9 and 11 of [BT04]. Dualizing the exact sequence

$$0 \rightarrow K^*/k^* \rightarrow \text{Div}(C) \rightarrow \text{Pic}(C) \rightarrow 0$$

we obtain the sequence

$$0 \rightarrow \mathbb{Z}_\ell \xrightarrow{\Delta_\ell} \mathcal{M}(C(k), \mathbb{Z}_\ell) \rightarrow \mathcal{G}_\ell^a \rightarrow \mathbb{Z}_\ell^{2g} \rightarrow 0, \quad (16)$$

with the identifications

- $\text{Hom}(\text{Pic}(C), \mathbb{Z}_\ell) = \Delta_\ell(\mathbb{Z}_\ell)$  (since  $J(k) = \text{Pic}^0(C)$  is torsion);
- $\mathcal{M}(C(k), \mathbb{Z}_\ell) = \text{Hom}(\text{Div}(C), \mathbb{Z}_\ell)$  is the  $\mathbb{Z}_\ell$ -linear space of maps from  $C(k) \rightarrow \mathbb{Z}_\ell$  (note that  $\text{Div}(C)$  can be viewed as the free abelian group generated by points in  $C(k)$ );
- $\mathbb{Z}_\ell^{2g} = \text{Ext}^1(J(k), \mathbb{Z}_\ell)$ .

The interpretation

$$\mathcal{G}_\ell^a = \text{Hom}(K^*/k^*, \mathbb{Z}_\ell), \quad (17)$$

arising from Kummer theory allows us to identify

$$\mathcal{G}_\ell^a \subset \mathcal{M}(C(k), \mathbb{Q}_\ell)/\text{constant maps} \quad (18)$$

as the  $\mathbb{Z}_\ell$ -linear subspace of maps  $\mu : C(k) \rightarrow \mathbb{Q}_\ell$  (modulo constant maps) such that

$$[\mu, f] \in \mathbb{Z}_\ell \text{ for all } f \in K^*/k^*.$$

Here  $[\cdot, \cdot]$  is the pairing:

$$\begin{aligned} \mathcal{M}(C(k), \mathbb{Q}_\ell) \times K^*/k^* &\rightarrow \mathbb{Q}_\ell \\ (\mu, f) &\mapsto [\mu, f] := \sum_c \mu(q) f_c, \end{aligned} \tag{19}$$

where  $\text{div}(f) = \sum_c f_c c$ . In this language, an element of an inertia subgroup  $\mathcal{I}_{\nu, \ell}^a \subset \mathcal{G}_\ell^a$  corresponds to a “delta”-map (constant outside the point  $c = c_\nu$ ). Each  $\mathcal{I}_{\nu, \ell}^a$  has a canonical (topological) generator  $\delta_{\nu, \ell}$  and the (diagonal) map  $\Delta \in \mathcal{M}(C(k), \mathbb{Q}_\ell)$  from (16) is given by

$$\Delta_\ell = \sum_{c \in C(k)} \delta_{c, \ell}.$$

Consider the abelian Galois group  $\mathcal{G}_{(p)}^a = \prod_{\ell \neq p} \mathcal{G}_\ell^a$ . Let  $\mathcal{I} = \{\mathcal{I}_c^a\}$  be the set of 1-dimensional valuation subgroups  $\mathcal{I}_c^a \subset \mathcal{G}^a$  corresponding to points  $c \in C(k)$ .

**Conjecture 9.1.** *Let  $C$  be a curve of genus  $\mathbf{g}(C) \geq 2$  over  $k = \bar{\mathbb{F}}_p$ . The pair  $(\mathcal{G}_{(p)}^a, \mathcal{I})$  determines the function field  $k(C)$ , modulo isomorphisms.*

**Remark 9.2.** This fails when  $\mathbf{g}(C) = 1$ . For any two elliptic curves over  $k$  the pairs  $(\mathcal{G}_{(p)}^a, \mathcal{I})$  are isomorphic. There are two types: supersingular curves with  $J\{p\} = 0$  (which are all isogenous) and ordinary curves.

We have the following partial result:

**Theorem 9.3.** *Let  $C, \tilde{C}$  be curves of genus  $\geq 2$  over  $k = \bar{\mathbb{F}}_p$ , with  $p > 2$ . Assume that there is an isomorphism of pairs*

$$(\mathcal{G}^a, \mathcal{I}) \xrightarrow{\sim} (\tilde{\mathcal{G}}^a, \tilde{\mathcal{I}}).$$

*Assume in addition that either*

- $J\{p\} = 0$  or
- $\mathbf{g}(C) > 4$ .

*Then there is an isogeny  $J \rightarrow \tilde{J}$  and*

$$\text{End}_k(J) \otimes \mathbb{Z}_\ell = \text{End}_k(\tilde{J}) \otimes \mathbb{Z}_\ell,$$

*for all  $\ell \neq p$ .*

The condition  $\mathbf{g}(C) > 4$  arises as follows: in the nonsupersingular case when  $J\{p\} \neq 0$ , our argument will be based on a detailed understanding of the map

$$\begin{aligned} j : C^{(2)} \times C^{(2)} &\rightarrow J \\ ((x, x'), (y, y')) &\mapsto (x + x') - (y + y'). \end{aligned}$$

In particular, it will be essential to describe all abelian varieties in the image of  $j$ . The corresponding classification is carried out in Section 10, under the assumption that  $\mathbf{g}(C) > 4$ .

*Proof of Theorem 9.3.* We will reduce to a version of Theorem 1.2, following closely the description of Galois groups in [BT04], Section 11.

Dualizing (17), we recover the pro- $\ell$ -completion  $\hat{K}_\ell^*$  of the multiplicative group  $K^*/k^*$  as  $\text{Hom}(\mathcal{G}_K^a, \mathbb{Z}_\ell)$ . Consider the following exact sequences

$$0 \rightarrow K^*/k^* \xrightarrow{\rho_C} \text{Div}^0(C) \xrightarrow{\varphi} J(k) \rightarrow 0, \quad (20)$$

$$0 \rightarrow K^*/k^* \otimes \mathbb{Z}_\ell \xrightarrow{\rho_{C,\ell}} \text{Div}^0(C) \otimes \mathbb{Z}_\ell \xrightarrow{\varphi_\ell} J\{\ell\} \rightarrow 0. \quad (21)$$

Put

$$\mathcal{T}_\ell(C) := \varprojlim \text{Tor}_1(\mathbb{Z}/\ell^n, J\{\ell\}).$$

We have  $\mathcal{T}_\ell(C) = \mathbb{Z}_\ell^{2\mathbf{g}}$ , where  $\mathbf{g}$  is the genus of  $C$ . Passing to pro- $\ell$ -completions in (20) we obtain an exact sequence of torsion-free groups

$$0 \rightarrow \mathcal{T}_\ell(C) \rightarrow \hat{K}_\ell^* \xrightarrow{\hat{\rho}_C} \widehat{\text{Div}^0(C)} \rightarrow 0, \quad (22)$$

since  $J(k)$  is an  $\ell$ -divisible group. We write  $\widehat{\text{Div}^0(C)}_\ell$  for the  $\ell$ -completion of  $\text{Div}^0(C)$ . Clearly,  $\text{Div}^0(C) \otimes \mathbb{Z}_\ell \subset \widehat{\text{Div}^0(C)}_\ell$  and we have a diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & K^*/k^* \otimes \mathbb{Z}_\ell & \xrightarrow{\rho_{C,\ell}} & \text{Div}^0(C) \otimes \mathbb{Z}_\ell & \xrightarrow{\varphi_\ell} & J\{\ell\} \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 \rightarrow \mathcal{T}_\ell(C) \rightarrow & \hat{K}_\ell^* & \xrightarrow{\hat{\rho}_{C,\ell}} & \widehat{\text{Div}^0(C)}_\ell & \xrightarrow{\hat{\varphi}_\ell} & 0. \end{array} \quad (23)$$

Fix a valuation  $\nu_0$  and a generator  $\delta_{\nu_0}$  of  $\mathcal{I}_{\nu_0}^a$ . This gives a canonical identification of generators  $\delta_\nu \in \mathcal{I}_\nu^a$  for all  $\nu \neq \nu_0$ , and similarly all  $\delta_{\nu,\ell} \in \mathcal{I}_{\nu,\ell}^a$ , for all  $\ell \neq p$ .

Let  $\mathcal{FS}(C)_\ell \subset \hat{K}_\ell^* = \text{Hom}(\mathcal{G}_\ell^a, \mathbb{Z}_\ell)$  be the subgroup topologically generated by elements  $\alpha_\ell \in \hat{K}_\ell^*$  such that

- $\alpha(\delta_{\nu_0,\ell}) = 1$ ,
- $\alpha(\delta_{\nu,\ell}) = -1$ , for some  $\nu \neq \nu_0$ .
- $\alpha_\ell$  is trivial on all  $\delta_{\nu',\ell}$ , for  $\nu' \neq \nu, \nu_0$ .

The group  $\mathcal{FS}(C)_\ell$  is equal to  $\text{Div}^0(C) \otimes \mathbb{Z}_\ell$  and we get a sequence

$$0 \rightarrow \mathcal{T}_\ell(C) \rightarrow \mathcal{FS}(C)_\ell \rightarrow J\{\ell\} \rightarrow 0, \quad (24)$$

with cohomology isomorphic to  $K^*/k^* \otimes \mathbb{Z}_\ell$ . Sequence (24) defines a map

$$C(k) \xrightarrow{\iota_\ell} J\{\ell\}.$$

Combining these, we obtain a map

$$\iota = \prod_{\ell \neq p} \iota_\ell : C(k) \rightarrow J(k)/J\{p\}.$$

If  $J\{p\} = 0$ , the map  $\iota$  is an embedding and we can apply Theorem 1.2 to conclude that the Galois isomorphism implies isogeny.

Assume that  $J\{p\} \neq 0$  and  $\mathbf{g}(C) > 4$ .

**Lemma 9.4.** Let  $C$  be a curve of genus  $\mathbf{g}(C) > 4$ . If  $j(C^{(2)} \times C^{(2)}) \cap J\{p\}$  is infinite then  $j(C^{(2)} \times C^{(2)}) \subset J$  contains a nontrivial abelian variety.

*Proof.* Consider the action of  $\mathbb{Z}_p$  generated by the  $p$ -component of some power of the Frobenius endomorphism. Under the assumptions, the  $\mathbb{Z}_p$ -orbits of points in  $j(C^{(2)} \times C^{(2)})$  can be arbitrarily large. Hence  $j(C^{(2)} \times C^{(2)})$  contains arbitrarily large subsets which are invariant under translations by big cyclic  $p$ -groups. Such subsets must be contained in translates of abelian subvarieties in  $J$  (see Remarks 5.8, 5.7 and [Box92]).  $\square$

*Case 1:  $j(C^{(2)} \times C^{(2)})$  does not contain a nontrivial abelian variety.*

By Lemma 9.4,  $j(C^{(2)} \times C^{(2)})(k) \cap J\{p\}$  is finite. Let  $k_0$  be a sufficiently large finite extension of the ground field such that  $J(k_0)$  contains all points  $x, x', y, y'$  with  $(x + x') - (y + y') \in J\{p\} - 0$ , and a finite subgroup  $A_p \subset J\{p\}$  with trivial action of  $\mathbb{Z}_p$  (generated by the Frobenius  $\text{Fr}$  over  $k_0$ ). We will also assume that  $A_p \supset J[p]$ . Put  $J_0 := J(k_0)$  and define inductively  $J_{n+1}$  as the subset of points  $x \notin J_n \oplus J\{p\}$  such that there is an  $x'$  with  $x + x' \in J_n \oplus J\{p\}$ . By induction, we obtain a subgroup  $J_\infty \subset J(k)$ . Note that  $J_\infty$  contains  $J(k_\infty)$ , where  $k_\infty$  is the 2-closure of  $k_0$ .

We claim that  $J(k_\infty)$  is closed under the above operation. Assume otherwise. The action of  $\mathbb{Z}_p$  on  $J(k_0)$  and hence on  $J(k_\infty)$  is trivial. Let  $x + x' + y_p \in J(k_\infty)$ , with  $y_p \in J\{p\} \setminus A_p$ . Then  $\mathbb{Z}_p$  acts nontrivially on  $y_p$  but trivially on  $x + x' + y_p$ . Thus  $\gamma(x + x') \neq x + x'$ , for some  $\gamma \in \mathbb{Z}_p$ , and  $\gamma(x + x') - (x + x') \in J\{p\}$ . However, by assumption all such points are contained in  $J(k_0)$ , where the action of  $\gamma \in \mathbb{Z}_p$  is trivial, contradiction.

In particular, if  $\tilde{C}$  is another curve with the same data and  $\tilde{J}(\tilde{k}_0)$  contains  $J(k_0)$  then we obtain a tower of inclusions of groups as in Lemma 7.9 and we can apply Theorem 7.10.

Let  $k_0$  be as above and assume that  $0 \neq x + x_1 \in J(k_0)/J\{p\}$  but that  $x, x_1 \notin J(k_1)$ . Then  $\gamma(x) + \gamma(x_1) = x + x_1 \neq 0$ , which implies that  $C$  is hyperelliptic and that  $x, x_1$  are conjugated by a hyperelliptic involution, hence  $0 = x + x_1$ , contradicting the assumption on  $x, x_1$ . Thus we can proceed as before.

*Case 2:  $j(C^{(2)} \times C^{(2)})$  contains a nontrivial abelian variety.*

Assume now that  $j(C^{(2)} \times C^{(2)})$  does contain an abelian variety. In Section 10 we give a classification of such subvarieties, when  $\mathbf{g}(C) > 4$ . By Corollary 10.4 there is a divisor  $D \subset C^{(2)}$  such that any abelian variety in  $j(C^{(2)} \times C^{(2)})$  is contained in the image of  $D \times C^{(2)} \cap C^{(2)} \times D$ . Thus there exist only finitely many pairs  $x, x' \in C$  and  $y, y' \in C$  with  $x + x' \notin D$  and  $y + y' \notin D$  and such that  $(x + x') - (y + y') \in J\{p\}$ . Let  $k_0$  be a sufficiently large finite field so that  $J(k_0)$  contains all such pairs  $x, x'$  and  $y, y'$  and so that  $x, \gamma(x) \in C(k_1)$  with  $x + \gamma(x) \notin D$  generate  $J(k_1)$ , for any finite extension  $k'/k_0$ . Then we can apply the same argument as above.

Note that such a field  $k_0$  exists, since the number of elements in  $D(k')$  grows as the square root of the number of elements in  $C(k')$ . Hence we can combine the arguments Lemma 5.2, 5.5 and 7.8 to show that for sufficiently large  $k_0$  our assumption holds. This finishes the proof of Theorem 9.3.  $\square$

**Remark 9.5.** When  $C$  has an algebraic automorphism  $\alpha$  such that  $C' = C/\alpha$  has genus  $1 \leq \mathbf{g}(C') \leq \mathbf{g}(C)/2$  we recover the algebraic projection  $C \rightarrow J' \subset J$ . In particular, we can recover every bielliptic involution.

For example, the Klein quartic curve is the unique curve of genus 3 with the maximal number of bielliptic involutions. Thus the algebraic structure of the Klein curve is completely encoded in the pair  $(\mathcal{G}^a, \mathcal{I})$ . Same holds for many other curves with sufficiently many maps onto curves of small genus, providing nontrivial examples where Conjecture 9.1 holds.

## 10. Appendix: Geometric background

In this section we work over an algebraically closed field  $k$  of characteristic  $\neq 2$ .

Let  $C$  be a curve of genus  $\mathbf{g}(C) \geq 2$  and  $J$  its Jacobian. We will identify the Jacobians of degree  $n$  zero-cycles  $J^n$  with  $J$ . Recall that a  $d$ -gonal structure on  $C$  is a surjective morphism  $C \rightarrow \mathbb{P}^1$  of degree  $d$ . A hyperelliptic structure on  $C$  is a surjective morphism  $C \rightarrow \mathbb{P}^1$  of degree 2 and a bielliptic structure a surjective morphism  $C \rightarrow E$  of degree 2. If  $W_2^1(C) \neq \emptyset$  then  $C$  is hyperelliptic and if  $W_3^1(C) \neq \emptyset$  and some element from  $W_3^1(C)$  defines a proper map then  $C$  is trigonal.

Consider the map

$$\begin{aligned} j : C^{(2)} \times C^{(2)} &\rightarrow J \\ ((x, x'), (y, y')) &\mapsto (x + x') - (y + y'). \end{aligned}$$

It contracts the diagonal  $\Delta = \Delta(C^{(2)})$  to a point and the divisor

$$\delta := \{((x, x'), (y, y')) \in C^{(2)} \times C^{(2)} \mid x' = y'\}$$

to a surface  $j(C \times C)$ . Denote the union of the diagonal and the divisor  $\delta$  above as  $D_\delta$ .

Assume that

$$j((x, x'), (y, y')) = j((z, z'), (w, w')),$$

and that  $(x, x') \neq (y, y')$  and  $(x, x') \neq (z, z')$  in  $C^{(2)}$ . If  $(x, x', w, w') \neq (z, z', y, y')$  as elements in  $C^{(4)}$  then the relation

$$((x + x') - (y + y')) - ((z + z') - (w + w')) = 0 \in J$$

gives a nontrivial relation of degree  $\leq 4$

$$(x + x' + w + w') - (z + z' + y + y').$$

Thus if there is a linear series  $L$  of degree  $\leq 4$  on  $C$  with  $H^0(C, L) \geq 2$ , i.e., the variety  $W_4^1(C)$  is nonempty.

**Lemma 10.1.** Assume that

- $(x, x', w, w') = (z, z', y, y')$  in  $C^{(4)}$ ,
- $((x, x'), (y, y')) \neq ((z, z'), (w, w'))$  in  $C^{(2)} \times C^{(2)}$ ,
- $(x, x') \neq (y, y')$  and  $(z, z') \neq (w, w')$  in  $C^{(2)}$ .

Then there is a set  $\{X, Y, Z, W\}$  which contains both sets  $\{x, x', y, y'\}, \{z, z', w, w'\}$  so that after some identification

$$((x, x'), (y, y')) = ((X, Y), (Y, Z)) \quad \text{and} \quad ((z, z'), (w, w')) = ((X, W), (W, Z)).$$

in  $C^{(2)} \times C^{(2)}$ . Hence  $\{x, x', y, y'\}, \{z, z', w, w'\} \in D_\delta = \Delta \cup \delta$ .

*Proof.* Since  $(x, x', w, w') = (z, z', y, y')$  in  $C^{(4)}$  the four-tuple  $\{x, x', w, w'\}$  contains also all the elements from  $\{z, z', y, y'\}$ . Thus if we denote  $\{x, x', w, w'\}$  as  $(X, Y, Z, W)$  and assume that none of the pairs  $((x, x'), (y, y')), ((z, z'), (w, w'))$  consists of the same letters we obtain that modulo permutation of  $(X, Y, Z, W)$

$$(x, x') = (X, Y), \quad (w, w') = (Z, W), \quad (z, z') = (Y, Z), \quad (y, y') = (W, X),$$

and that the above identification is the only possible, modulo permutations. Thus  $\{x, x', y, y'\}, \{z, z', w, w'\} \in D_\delta = \Delta \cup \delta$ .  $\square$

The following theorem classifies 4-gonal structures on  $C$ .

**Theorem 10.2** (Mumford, cf. [ACGH85], p. 193). *Assume that  $W_4^1(C) \neq \emptyset$ . Then one of the following holds:*

- (0)  $\dim W_4^1(C) = 0$ : then  $C$  has a finite number of 4-gonal structures;
- (1)  $\dim W_4^1(C) = 1$ :
  - (a)  $C$  is smooth plane curve of genus 6 and degree 5 and the corresponding line bundle  $L = H - p$ ,  $p \in C$ , where  $H$  is a hyperplane section;
  - (b)  $C$  is bielliptic and  $L$  is obtained from a bielliptic involution  $C \rightarrow E \rightarrow \mathbb{P}^1$ , where the second map arises from a reflection with respect to some point on  $E$ ;

- (c)  $C$  is trigonal with a unique trigonal structure and  $L = H + c$ , where  $c \in C(k)$ , and  $H$  defines a trigonal map onto  $\mathbb{P}^1$ ;
- (2)  $\dim W_4^1(C) = 2$ : then  $C$  is hyperelliptic and  $L = 2H$ , where  $H$  is a hyperelliptic bundle, or  $L = H + c + c'$ , where  $c, c' \in C(k)$  and  $c' \neq \sigma(c)$ , for the hyperelliptic involution  $\sigma$ ; in the former case,  $\dim H^0(C, 2H) = 3$  and any other  $L$  as above defines the same projection  $H$ .

Mumford's theorem holds over arbitrary ground fields. We use it to describe explicitly abelian subvarieties of  $j(C^{(2)} \times C^{(2)}) \subset J$ , for  $g(C) > 4$ .

**Theorem 10.3.** *Let  $C$  be a curve of genus  $g(C) > 4$  and  $J$  its Jacobian. Assume that  $j(C^{(2)} \times C^{(2)}) \subset J$  contains translations of abelian subvarieties. Then one of the following holds.*

1.  $C$  is hyperelliptic with a map  $C \rightarrow E$  of degree 4 and

$$E \subset W_4 = j(C^{(2)} \times C^{(2)}).$$

2.  $C$  is hyperelliptic with a map  $C \rightarrow E$  of degree 3 and  $E \times C \subset W_4(C) \subset J$ , with the map corresponding to the summation of cycles. Further,  $E \subset W_3(C) \subset J$ , with the embedding induced by the projection from  $C$ .
3.  $C$  is bielliptic and there is a finite number of bielliptic structures  $e_i : C \rightarrow E_i$ . Each such map defines an embedding  $i_2 : E_i \subset C^{(2)}$ . The abelian subvarieties are:
  - $j(E_i \times E_i) = E_i \subset j(C^{(2)} \times C^{(2)})$  (of dimension one),
  - $j(E_i \times E_{i'}) \subset j(C^{(2)} \times C^{(2)})$ , with  $i \neq i'$ , (of dimension two), and
  - $j(E_i \times C^{(2)})$  - two-dimensional families of elliptic curves.
4.  $C$  admits a map  $h : C \rightarrow \tilde{C}$  of degree two onto a curve of genus 2, and  $A = \tilde{C}^{(2)}$ .

**Corollary 10.4.** *There is a divisor  $D \subset C^{(2)}$  such that abelian subvarieties in  $j(C^{(2)} \times C^{(2)})$  are contained in  $j(D \times C^{(2)} \cup C^{(2)} \times D)$ . In the hyperelliptic cases 1 and 2, the components of  $D$  are defined by the curves of two-cycles of degree 4 and 3 maps. In Case 3, a bielliptic structure defines an elliptic curve in  $C^{(2)}$  which is a component of  $D$ . In Case 4, a component is given by  $\tilde{C}$  of genus 2 embedded into  $C^{(2)}$ .*

The remainder of this Appendix is devoted to a proof of Theorem 10.3. We use the results and techniques from [AH91].

First we consider the case when  $C$  is hyperelliptic. Then  $j(C^{(2)} \times C^{(2)}) \subset J$  coincides with  $W_4(C)$ , the image of  $C^{(4)}$ .

**Lemma 10.5.** *Let  $C$  be a hyperelliptic curve of genus  $g(C) > 4$ . If  $W_4(C)$  contains a nontrivial abelian subvariety  $A$  then:*

1.  $\dim A = 1$  and there is a surjective map  $f : C \rightarrow A$  of degree 3 or 4, and the embedding of  $A$  into  $W_3(C)$ , resp.  $W_4(C)$ , is induced by this map.

2. There is a surjective map  $f : C \rightarrow \tilde{C}$  of degree 2, where  $g(\tilde{C}) = 2$ , and  $A = \tilde{C}^{(2)}$ .

*Proof.* By Theorem 4 of [AH91], if  $A \subset W_3(C)$  is an abelian subvariety and  $g(C) > 4$  then  $A$  is an elliptic curve and  $C$  admits a map  $C \rightarrow A$  of degree  $\leq 3$ , which defines the embedding of  $A$  into  $W_3(C)$ .

Let  $A \subset W_4(C)$  be an abelian variety. Let  $A_2 = A + (a) \subset W_8(C)$  be the translation of  $A$  by an  $a \in A(k)$ . Each  $\alpha \in A_2(k)$  defines a line bundle  $L_\alpha$  on  $C$  (of degree 8). By Lemma 1 in [AH91],

$$\dim H^0(C, L_\alpha) > \dim A + 1.$$

By Lemma 2 in [AH91], if  $\dim H^0(C, L_\alpha) = 2$  then  $A$  has dimension 1 and there is a map  $C \rightarrow A$  of degree 4.

Now assume that  $\dim H^0(C, L_\alpha) \geq 3$ , for all  $\alpha$ . Then  $8 \leq 2g(C) - 2$ . Since  $C$  is hyperelliptic the map

$$\phi_\alpha : C \rightarrow \mathbb{P}^{r(\alpha)},$$

where  $r(\alpha) = \dim H^0(C, L_\alpha) - 1$ , is not birational onto its image. Thus  $C$  satisfies the assumptions of Lemma 3 [AH91] and we conclude that either  $A \subset W_d^1(C)$ , where  $2 \leq d \leq 4$ , or there is a nontrivial factorization

$$C \xrightarrow{\rho} \tilde{C} \rightarrow \mathbb{P}^{r(\alpha)}$$

and an embedding  $A \subset W_{\tilde{d}}(\tilde{C})$ , with  $\tilde{d} = 4/\deg(\rho)$ . Since  $C$  is hyperelliptic,

$$W_4^1(C) = W_3^1(C) = W_2(C).$$

We now apply Theorem 3 [AH91]: if  $A \subset W_2(C)$  and  $g(C) \geq 3$  then  $C$  is not hyperelliptic, contradiction to our assumption. If  $\tilde{d} = 1$  then  $A \subset W_1(\tilde{C})$  and hence  $\tilde{C} = A$  is an elliptic curve and we are in Case 1.

If  $\tilde{d} = 2$ , then  $A \subset W_2(\tilde{C})$  and either  $1 \leq g(\tilde{C}) \leq 2$  or  $\tilde{C}$  is bielliptic. If  $\tilde{C}$  were bielliptic we would get a degree 4 map from  $C$  onto an elliptic curve. If  $g(\tilde{C}) = 1$  then  $C$  is bielliptic, contradicting the assumption on the genus of  $C$ . If  $g(\tilde{C}) = 2$  then  $A = W_2(\tilde{C})$ .  $\square$

From now on we assume that  $C$  is nonhyperelliptic. In particular,  $C^{(2)}$  does not contain rational curves.

Assume that the map  $j : C^{(2)} \times C^{(2)} \rightarrow J$  is an embedding outside of the diagonal  $\Delta \cup \delta$ . Then  $A \subset j(C^{(2)} \times C^{(2)})$  lifts birationally to  $C^{(2)} \times C^{(2)}$  and the image of  $A$  in each projection to  $C^{(2)}$  must be an elliptic curve or a point. It follows that  $A$  is contained in a product of elliptic curves in  $C^{(2)} \times C^{(2)}$ . It remains to apply the following lemma (see, e.g., [AH91]).

**Lemma 10.6.** Assume that  $C$  is a nonhyperelliptic curve of genus  $g(C) > 4$ . Let  $\tilde{C} \subset C^{(2)}$  be a curve of genus 1 or 2. Then there is a degree 2 map  $C \rightarrow \tilde{C}$ .



Now we assume that there is a nontrivial subvariety  $Z \subset C^{(2)} \times C^{(2)}$  not contained in the diagonal  $\Delta(C^{(2)})$  such that  $j : Z \rightarrow J$  is not an embedding on the complement of  $\Delta(C^{(2)})$ . This occurs only when  $C$  is one of the curves satisfying Mumford's theorem 10.2. In particular,  $W_4^1(C) \neq \emptyset$ .

A map  $f : C \rightarrow \mathbb{P}^1$  of degree 4 determines a possibly reducible curve

$$C_f := (C \times_{\mathbb{P}^1} C \setminus \Delta(C)) / \mathbb{Z}/2,$$

where the  $\mathbb{Z}/2$ -action interchanges the factors. The curve  $C_f$  parametrizes unordered pairs of points  $(c, c')$  in the fibers of  $f$ . We have a natural embedding  $\xi_f : C_f \subset C^{(2)}$  and a projection  $\eta_f : C_f \rightarrow \mathbb{P}^1$  of degree 6. In addition, there is a natural nontrivial fiberwise involution  $\iota : C_f \rightarrow C_f$  which maps the degree 2 cycle  $(c, c')$  into the complementary cycle in the same fiber of  $f$ , i.e., if  $(c, c', c'', c''')$  is a fiber of  $f$  then  $\iota(c, c') = (c'', c''')$ . The map  $g : C_f / \iota = C_g \rightarrow \mathbb{P}^1$  has degree 3. The curve  $C_g$  parametrizes the splittings of the fibers of  $f$  into a pairs of degree 2 zero-cycles.

Let  $n_2, n_{2,2}, n_3, n_4$  be the number of different ramification types for  $f : C \rightarrow \mathbb{P}^1$ , i.e.,  $n_i$  is the number of fibers of  $f$  with one ramification of multiplicity  $i$ , for  $i = 2, 3, 4$ , and  $n_{2,2}$  the number of fibers with 2 simple ramifications.

**Lemma 10.7.** Assume one of the following holds:

- $C_f$  is irreducible and at least one of the  $n_2, n_3$  or  $n_4$  is nonzero or
- $C_f$  is reducible and  $f : C \rightarrow \mathbb{P}^1$  is not a Galois covering.

Then

$$g(C_g) \geq \frac{1}{2}g(C) \geq 3.$$

*Proof.* The Galois group  $\text{Gal}(f)$  of the 4-covering  $f : C \rightarrow \mathbb{P}^1$  is one of the following

$$\mathfrak{S}_4, \mathfrak{A}_4, \mathfrak{D}_4, \mathbb{Z}/4, \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

The curve  $C_f$  is irreducible iff  $\text{Gal}(f)$  acts transitively on the subsets of 6 unordered pairs of 4 points. This is the case of  $\mathfrak{S}_4, \mathfrak{A}_4$ . In the case of  $\mathfrak{D}_4$  and  $\mathbb{Z}/4$  the set of 6 unordered pairs splits into two orbits of orders 4 and 2, respectively, and in the case of  $\mathbb{Z}_2 \oplus \mathbb{Z}/2$  there are orbits of order 2. This determines all possible splittings of  $C_f$ .

Note that for  $\mathfrak{D}_4, \mathbb{Z}/4$  the curve  $C$  is isomorphic to a connected component of  $C_f$  and there is a natural involution  $\theta$  on  $C$  given by a central element of order 2 in  $\mathfrak{D}_4$  and  $\mathbb{Z}/4$ , respectively. The quotient hyperelliptic curve  $C/\theta$  coincides with the second component of  $C_f$ , so that  $C_f = C \cup C/\theta$ .

It is easy to obtain numerical characteristics of  $C_f$  and  $C_g$  in all cases. By Hurwitz' formula,

$$2g(C) - 2 = n_2 + 2n_{2,2} + 2n_3 + 3n_4 - 8. \quad (25)$$

There is a natural correspondence between the ramification diagrams for the fibers of  $C, C_g$  and  $C_f$ . Write  $(i_1, \dots, i_r)$  for the ramification type of a fiber of the corresponding map to  $\mathbb{P}^1$ , a smooth fiber of a map of degree  $r$  corresponds to  $(1, \dots, 1)$ ,  $r$ -times. We have

$C$	$C_g$	$C_f$
$(1, 1, 1, 1)$	$(1, 1, 1)$	$(1, 1, 1, 1, 1, 1)$
$(2, 1, 1)$	$(2, 1)$	$(2, 2, 1, 1)$
$(2, 2)$	$(2, 1)$	$(4, 1, 1)$
$(3, 1)$	$(3)$	$(3, 3)$
$(4)$	$(3)$	$(6)$

Note that the action of  $\mathbb{Z}/2$  on the fibers of  $C_f$  is free only in the first and third cases. We obtain

$$g(C_g) = \frac{1}{2}n_2 + \frac{1}{2}n_{2,2} + n_3 + n_4 - 2.$$

Using (25),

$$2g(C_g) = n_2 + n_{2,2} + 2n_3 + 2n_4 - 4 > \frac{1}{2}n_2 + n_{2,2} + n_3 + \frac{3}{2}n_4 - 3 = g(C)$$

and

$$\frac{1}{2}n_2 + n_3 + \frac{1}{2}n_4 - 1 = 2g(C_g) - g(C)$$

and hence  $g(C_g) \geq 3$ , if either  $g(C) > 5$  or some singular fibers of  $f$  are not of type  $(2, 2)$ . Note that if the action of  $\mathbb{Z}/2$  is free on  $C_f$  then  $n_{2,2} = 0$  and  $g(C_g) = g(C) + 1 > 5$ .

Consider the reducible case with the Galois group  $\mathfrak{D}_4$ . As explained above,  $C$  is obtained as a quotient of the Galois cover by a noncentral  $\mathbb{Z}/2 \subset \mathfrak{D}_4$ . Thus there is also an action of a central  $\mathbb{Z}/2$  on  $C$ . The family of degree two cycles splits into a curve  $C$  and  $C/\mathbb{Z}/2$ . The only singular fibers are  $(2, 1, 1), (2, 2), (4)$  and the corresponding fibers or  $(1, 1), (2), (2)$ , respectively. Thus  $C_g$  is a hyperelliptic curve and  $C_f$  is a double covering with ramifications over points in  $C_g$  with some of them not belonging to the invariant points of the hyperelliptic involution. If the Galois group is  $\mathbb{Z}/4$  then  $C_f$  is a double covering of  $C_g$ , doubly ramified over ramification points of  $C_g \rightarrow \mathbb{P}^1$ . This gives a lower bound on the genus of  $C_g$ :

$$g(C) = \frac{3}{2}n_4 - 5 \quad \text{and} \quad g(C_g) = n_4 - 1.$$

Thus

$$2g(C_g) > g(C).$$

When  $\text{Gal}(f) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$  the curve  $C$  is actually a fiber product of two hyperelliptic curves over  $\mathbb{P}^1$ .  $\square$

We continue the investigation of  $Z$ . Consider the map

$$C_f \times C_f \xrightarrow{\xi_f^2} C^{(2)} \times C^{(2)} \xrightarrow{j} J.$$

There is natural action of  $\mathfrak{D}_4$  on  $C_f \times C_f$  which contains the permutation of fibers  $i$  and fiberwise involutions  $(\iota, id), (id, \iota)$  on  $C_f \times C_f$ .

**Lemma 10.8.** Let  $f : C \rightarrow \mathbb{P}^1$  be a map of degree 4. The restriction of  $j$  to the image  $\xi_f^2(C_f \times C_f)$  is the composition of the quotient by the involution  $i \circ (\iota, \iota)$ , which is conjugate to  $i$ , with a birational embedding, which is an isomorphism onto its image on the complement to the diagonal  $\Delta(C^{(2)})$  and

$$\bigcup_{f' \neq f} \xi_{f'}^2(C_{f'} \times C_{f'}) \subset C^{(2)} \times C^{(2)},$$

over all other 4-gonal maps  $f'$ . In particular, we have a factorization

$$\begin{array}{ccc} C_f \times C_f & \xrightarrow{\xi_f^2} & C^{(2)} \times C^{(2)} \\ \downarrow & & \downarrow j \\ C_f^{(2)} & \xrightarrow{j_f} & J. \end{array}$$

*Proof.* Consider the pair of cycles  $(x_1, x_2), (y_1, y_2) \in C_f \times C_f$ . Then

$$(x_1 + x_2) - \iota(y_1, y_2) = y_1 + y_2 - \iota(x_1, x_2)$$

which implies that  $j$  factors through the quotient by  $i \circ (\iota, \iota)$  and hence  $C_f \times C_f \subset Z$ . Assume that

$$(x_1 + x_2) - (z_1 + z_2) = (y_1 + y_2) - (w_1 + w_2),$$

where  $(z_1 + z_2) \neq \iota(y_1, y_2)$ . Since  $C$  is nonhyperelliptic,

$$(z_1 + z_2) \neq (x_2 + x_3), (x_2, x_3) = \iota(x_1, x_2)$$

and we obtain

$$y_1 + y_2 + z_1 + z_2 = x_1 + x_2 + w_1 + w_2$$

which corresponds to a different 4-gonal structure  $f'$  on  $C$  with  $(x_1, x_2), (y_1, y_2) \subset C_{f'} \times C_{f'}$ .  $\square$

**Corollary 10.9.** *If  $C_f$  is irreducible then for any other  $C_{f'}$  the intersection*

$$\xi_f^2(C_f \times C_f) \cap \xi_{f'}^2(C_{f'} \times C_{f'})$$

*is finite. Hence the image  $j \circ \xi_f^2(C_f \times C_f)$  is birational to  $C_f^{(2)}$ .*

*Proof.* Mumford's theorem 10.2 implies that there is at most a one-dimensional family of 4-gonal structure on  $C$ . Hence the intersection of  $\xi_f^2(C_f \times C_f)$  with the union of  $\xi_{f'}^2(C_{f'} \times C_{f'})$ , over all other 4-gonal structures  $f'$ , is at most a curve in  $\xi_f^2(C_f \times C_f)$ .  $\square$

**Lemma 10.10.** Let  $Z^\circ \subset C^{(2)} \times C^{(2)} \setminus \Delta(C^{(2)})$  be the maximal subvariety such that  $j$  restricted to  $Z^\circ$  is not an isomorphism onto its image. Let  $Z$  be the Zariski closure of  $Z^\circ$  in  $C^{(2)} \times C^{(2)}$ . Then

$$Z = \cup_f Z_f,$$

over the set of 4-gonal structures on  $C$ . Here  $Z_f = C_f \times C_f$ .

*Proof.* Assume that

$$j((x, x_1), (y, y_1)) = j((y_2, y_3), (x_2, x_3)).$$

Then

$$(x + x_1) - (y + y_1) = (y_2 + y_3) - (x_2 + x_3)$$

and hence

$$(x + x_1) + (x_2 + x_3) = (y + y_1) + (y_2 + y_3)$$

which means that for any  $z, w \in C^{(2)} \times C^{(2)}$ ,  $z \neq w$  with  $j(z) = j(w)$  there is a 4-gonal map  $f$  so that  $z, w \in C_f \times C_f$  and  $i(\iota, \iota)(z) = w$ .  $\square$

**Corollary 10.11.** *If  $C$  is not hyperelliptic then  $j : C^{(2)} \times C^{(2)} \rightarrow J$  is a birational isomorphism onto its image.*

*Proof.* Indeed, Mumford's theorem 10.2 implies that the family of 4-gonal maps on  $C$  is at most one-dimensional. Hence  $Z_f$  has dimension 2 for any 4-gonal structure. Since we have at most  $W_4^1(C)$  in the nonhyperelliptic case,  $Z$  is at most a one-dimensional family of surfaces and the map  $j$  is an embedding outside of  $Z$  and  $\delta$ . Thus  $j$  is a birational isomorphism onto its image.  $\square$

**Lemma 10.12.** Any abelian subvariety  $A \in j(C^{(2)} \times C^{(2)})$  which is not in  $j(Z)$  is contained in either  $j(E_1 \times C^{(2)})$  or  $j(C^{(2)} \times E_1)$ , where  $E_1 \subset C^{(2)}$  is an elliptic curve. This embedding corresponds to a bielliptic structure  $h_1 : C \rightarrow E_1$ .

*Proof.* Let  $A \in j(C^{(2)} \times C^{(2)}) \setminus j(Z)$ . Then  $j^{-1}(A) = \tilde{A}$  is birationally isomorphic to  $A$ . The projections  $\pi_1, \pi_2 : \tilde{A} \rightarrow C^{(2)}$  map it either into an elliptic curve  $E_i$  or into a point. Indeed, by assumption on  $C$  the surface  $C^{(2)}$  is of general type and does not contain a rational curve since  $C$  is not hyperelliptic. Thus the image  $\pi_i(A)$ ,  $i = 1, 2$ , is an elliptic curve for at least one  $i = 1, 2$ , for example  $\pi_1$ . By Theorem 10.3,  $C$  is bielliptic with an embedding  $E_i \hookrightarrow C^{(2)}$  corresponding to the bielliptic structure  $h_i : C \rightarrow E_i$ . Thus  $A \subset E_1 \times C^{(2)}$ .  $\square$

**Corollary 10.13.** *If  $A \subset j(C^{(2)} \times C^{(2)})$  does not correspond to Case 3 of Theorem 10.3 then  $A \subset j(Z)$ .*

Let us consider individual subvarieties  $Z_f \subset Z$ .

**Lemma 10.14.** *Let  $C$  be nonhyperelliptic, of genus  $g(C) > 4$ . Then the irreducible curve  $C_f$  is not bielliptic.*

*Proof.* Assume that  $C_f$  is bielliptic. Then  $C_g$  is also bielliptic. Indeed, consider the bielliptic map  $C_f \rightarrow E$ . There is a degree 4 surjective map  $C_f^{(2)} \rightarrow C_g^{(2)}$  which maps an elliptic curve  $E \subset C_f^{(2)}$  to an elliptic or a rational curve. In the second case, the involution on  $C_f$  maps to a hyperelliptic involution on  $C_g$ .

$$\begin{array}{ccc} C_f & \longrightarrow & E \\ \downarrow & & \downarrow \\ C_g & \longrightarrow & \mathbb{P}^1 \end{array}$$

If  $C_f, C_g$  are irreducible then  $C_g$  is trigonal. Hence  $g(C_g) \leq 2$ . However, by Lemma 10.7,  $g(C_g) \geq 3$ , contradiction. Thus the image of  $E$  is an elliptic curve and the diagram is:

$$\begin{array}{ccc} C_f & \longrightarrow & E \\ \downarrow & & \downarrow \\ C_g & \longrightarrow & \tilde{E} = E/\mathbb{Z}/2, \end{array}$$

where  $E \rightarrow \tilde{E}$  is an unramified covering of degree 2. Thus  $C_g$  is bielliptic and trigonal and  $C_f \rightarrow C_g$  is an unramified double cover induced by  $E \rightarrow \tilde{E}$ .

This implies that  $g(C_g) \geq 4$ . Indeed, if the trigonal structure  $C_g \rightarrow \mathbb{P}^1$  were invariant with respect to the bielliptic involution  $\iota$  then the latter would induce an involution  $\iota'$  on  $\mathbb{P}^1$ . Since  $\iota'$  has exactly two invariant points all the invariant points of  $\iota$  are contained in two fibers of the map  $C_g \rightarrow \mathbb{P}^1$ . Thus  $C_g$  is a degree 2 covering of  $\tilde{E}$  ramified in at most 6 points which implies the result. If on the other hand,  $C_g \rightarrow \mathbb{P}^1$  is not  $\iota$ -invariant then  $C$  has 3 different trigonal structures and hence maps birationally into a curve of bi-degree  $(3, 3)$  in  $\mathbb{P}^1 \times \mathbb{P}^1$ . Then

$$2g(C_g) - 2 \leq 3(H_1 + H_2)(H_1 + H_2) = D(D + K) = 6$$

and hence  $g \leq 4$ . Note that the genus of  $C$  is equal to  $g(C_g) - 1$  which follows from (25) because of the absence of 2, 2 and 4 fibers in this case. This finishes the proof of the lemma.  $\square$

**Remark 10.15.** The construction above is part of the classical Prym variety construction with  $J = \text{Prym}(C_g, \theta)$ , where  $\theta$  is a point of order two defining the nonramified covering  $C_f$ . Thus

$$g(C) = \dim \text{Prym}(C_g, \theta) = g(C_g) - 1.$$

**Lemma 10.16.** If  $C$  is not a plane curve of degree 5 then any abelian subvariety in the image  $j(C^{(2)} \times C^{(2)}) \subset J$  is contained in  $\bigcup_f Z_f$ , over all  $f$  defining 4-gonal structures on  $C$ , with reducible  $C_f$ .

*Proof.* If  $C_f$  is irreducible then  $C^{(2)}$  does not contain an elliptic curve by Lemma 10.14. The set where the map is not bijective coincides with the intersection locus with other  $C_{f'} \times C_{f'}$ . Since under the assumption of the lemma there is only a finite number of 4-gonal structures which don't correspond to a bielliptic structure, the one-dimensional families of  $C_{f'}$  correspond to bielliptic maps. They define the only curves in  $C^{(2)}$  where

$$j_f : C_f^{(2)} \setminus \Delta(C_f) \rightarrow J$$

is not an isomorphism. Thus only reducible  $C_f$  contribute abelian subvarieties in the image.  $\square$

**Lemma 10.17.** If  $C_f$  is reducible and  $j(Z_f)$  contains an abelian subvariety then:

1.  $C$  is bielliptic and  $f : C \rightarrow \mathbb{P}^1$  is a composition  $C \rightarrow E$  with an involution on  $E$ . Then  $C_f^{(2)}$  contains  $E$ .
2. The map  $f : C \rightarrow \mathbb{P}^1$  is a composition of a degree two map  $C \rightarrow \tilde{C}$  onto a curve of genus two and a hyperelliptic projection  $\tilde{C} \rightarrow \mathbb{P}^1$ . In this case  $j(Z_f)$  contains the abelian surface  $j(\tilde{C}^{(2)})$ .
3. If  $\mathbb{Z}/2 \oplus \mathbb{Z}/2$  acts on  $C$  then we get a combination of the above two cases, depending on the genus of the curves  $C_i$ .

*Proof.* It is evident that in all of these cases there is an abelian subvariety in  $j(Z_f)$ . In cases  $\mathfrak{D}_4, \mathbb{Z}/4$  the image of  $j(Z_f)$  is a birational embedding for three surfaces

$$C^{(2)}, (C/\theta)^{(2)}, C \times (C/\theta)$$

into  $J$ . Thus if  $C$  is not bielliptic the abelian subvariety may be contained in  $C \times (C/\theta)$  (and then  $C/\theta$  is an elliptic curve - contradicting the assumption) or in  $(C/\theta)^{(2)}$ . The latter is hyperelliptic and hence  $(C/\theta)^{(2)}$  does not contain elliptic curves if  $\mathbf{g}(C/\theta) \geq 3$ . Thus the only possibility is  $\mathbf{g}(C/\theta) = 2$  and  $(C/\theta)^{(2)}$  is birational to an abelian surface.

Similarly, in the case of  $\mathbb{Z}/2 \oplus \mathbb{Z}/2$  we have a union of  $C_i \times C_{i'}, i \neq i'$  and  $C_i^{(2)}$  which implies the result.  $\square$

Thus we have shown that unless  $C$  is a smooth plane curve of degree 5 and genus 6 the abelian subvariety is contained in  $j(Z)$  only in the cases described by the theorem.

**Lemma 10.18.** Let  $C \subset \mathbb{P}^2$  be a smooth plane curve of degree 5. Fix a point  $c \in C$ . Let  $f = f_c$  be the 4-gonal structure on  $C$  defined by projection from  $c$ . Then

1.  $Z$  is irreducible,
2.  $Z$  contains an open subvariety  $Z_0 \subset Z$  such that any point in  $Z_0$  is contained in a unique  $Z_{f_c}$ ,

3. there is a rational map  $\pi_f : Z \rightarrow C$  with the closures of a fiber  $\pi_f^{-1}(c) = C_{f_c} \times C_{f_c}, c \in C$ ,
4. the map  $j$  on  $Z_0$  has degree 2,
5. the map  $j$  on  $Z_0$  commutes with  $\pi_f$  and there is a commutative diagram of maps

$$\begin{array}{ccc} Z & \xrightarrow{\pi_f} & C \\ j \downarrow & & \parallel \\ j(Z) & \longrightarrow & C, \end{array}$$

6. any abelian subvariety  $A \subset j(C^{(2)} \times C^{(2)})$  is contained in  $j(Z_{f_c})$  for some  $c \in C$ .

*Proof.* We have already proved that any abelian subvariety in  $j(C^{(2)} \times C^{(2)})$  is contained in  $j(Z) = \bigcup j(Z_{f_c})$  since in the case of a smooth curve of degree 5 any linear series in  $W_4^1(C)$  corresponds to one of the four-gonal maps  $f_c, c \in C$ .

First we show that  $Z \subset C^{(2)} \times C^{(2)}$  is irreducible. As we have mentioned  $Z$  is a union of varieties  $C_{f_c} \times C_{f_c}, c \in C$ . It suffices to show that a generic curve  $C_{f_c}$  is irreducible. If  $C_{f_c}$  is not irreducible then by Lemma 10.17 there is a  $\mathbb{Z}/2$  action on  $C$ , with center  $c$  of the projection  $f_c$  fixed by this action. The structure of a smooth projective curve of degree 5 is unique on  $C$  and hence the group  $\mathbb{Z}/2$  above is a subgroup of a finite subgroup  $I_C \subset \text{PGL}_3(k)$  which stabilizes  $C \subset \mathbb{P}^2$ . Since there is only a finite number of subgroups  $\mathbb{Z}/2 \in I_C$ , the a number of projections  $f_c$  such that  $C_{f_c}$  is reducible is also finite. Hence  $Z$  is irreducible.

Any two-cycle  $(x, x_1)$  on  $C$  defines a unique line  $\mathfrak{l}(x, x_1)$  with  $\mathfrak{l}(x, x_1) \cap C$  containing  $(x, x_1)$ . When  $x, x_1$  are different,  $\mathfrak{l}(x, x_1)$  is the unique line through  $x, x_1$ . When  $x = x_1$  then  $\mathfrak{l}(x, x_1) = \mathfrak{l}(x, x)$  is the tangent to the smooth curve  $C$  at  $x \in C$ . Let  $((x, x_1), (y, y_1))$  be a point in  $Z$ .

If  $\mathfrak{l}(x, x_1) \neq \mathfrak{l}(y, y_1)$  then  $\mathfrak{l}(x, x_1), \mathfrak{l}(y, y_1)$  intersect at a unique point  $c \in C$ . This defines a rational surjective map

$$\begin{aligned} \pi_f : C^{(2)} \times C^{(2)} &\rightarrow C \\ ((x, x_1), (y, y_1)) &\mapsto c := \mathfrak{l}(x, x_1) \cap \mathfrak{l}(y, y_1) \end{aligned}$$

from an open subvariety  $Z^\circ \subset Z$ , defined by  $\mathfrak{l}(x, x_1) \neq \mathfrak{l}(y, y_1)$ . If  $\mathfrak{l}(x, x_1) = \mathfrak{l}(y, y_1)$  then the points  $x, x_1, y, y_1$  belong to the same 5-cycle in the intersection  $\mathfrak{l}(x, x_1) \cap C$ . If  $x + x_1 + y + y_1$  is the fiber of  $f_c$  defined by the fifth point  $c$  in the intersection  $\mathfrak{l}(x, x_1) \cap C$  then  $\pi_f((x, x_1), (y, y_1)) = c$  and hence  $\pi_f$  is well-defined on such  $((x, x_1), (y, y_1)) \in Z$ .

Thus  $\pi_f$  may fail to be well-defined only on the surface

$$S_{\mathfrak{l}} = \{((x, x_1), (x, x_2)) \in Z, \mid \mathfrak{l}(x, x_1) = \mathfrak{l}(x, x_2)\}.$$

Consider the restriction of  $j$  on  $Z_0 = Z \setminus S_{\mathfrak{l}}$ . Let us show that  $j$  is exactly of degree 2 on  $Z_0$  and  $j(S_{\mathfrak{l}}) \subset j(C \times C)$ , where  $C \subset J = J^1$  is a standard embedding.

Indeed, assume that  $((x, x_1), (y, y_1)) \in Z_0$ . Then they define a unique point  $c$  which is either the intersection point  $\mathbb{I}(x, x_1) \cap \mathbb{I}(y, y_1)$  or the the fifth point in the intersection  $\mathbb{I}(x, x_1) = \mathbb{I}(y, y_1) \cap C$ . The equality of zero-cycles

$$(x + x_1) - (w + w_1) = (y + y_1) - (z + z_1)$$

implies

$$(x + x_1) + (z + z_1) = (y + y_1) + (w + w_1).$$

Thus if  $\mathbb{I}(x, x_1) \neq \mathbb{I}(y, y_1)$  then  $\mathbb{I}(x, x_1) = \mathbb{I}(z, z_1), \mathbb{I}(y, y_1) = \mathbb{I}(w, w_1)$ . Hence  $\iota_{f_c}(x, x_1) = \iota_{f_c}(y, y_1)$ . We also have  $\pi_f((x, x_1), (y, y_1)) = \pi_f((w, w_1), (z, z_1))$  which yields the result in this case.

In the second case,  $(x + x_1) - (x_2 + x_3) = (z_1 + z_2) - (w_1 + w_2)$  implies  $(x + x_1) + (w_1 + w_2) = (x_2 + x_3) + (z_1 + z_2)$  and that  $\mathbb{I}(w_1, w_2) = \mathbb{I}(x_1, x_2), \mathbb{I}(z_1, z_2) = \mathbb{I}(x_2 + x_3)$ . Hence both cycles are contained in  $\mathbb{I}(x, x_1)$ . Unless  $(w_1, w_2) = (x_2, x_3)$  and  $(z_1, z_2) = (x, x_1)$  there is a relation between two positive cycles from  $\mathbb{I}(x, x_1) \cap C$  of degree  $< 4$  which cannot happen since  $C$  is neither trigonal, nor hyperelliptic. Thus we showed that the map  $j : Z_0 \rightarrow j(Z_0)$  is a map of degree 2. If  $((x, x_1), (x, x_2)) \in S_1$  then

$$j((x, x_1), (x, x_2)) = x_1 - x_2 \in j(C \times C).$$

This completes the description of the map  $j$  on  $Z$ .

Thus  $j$  commutes with the map  $\pi_f$  on  $Z_0$  and defines a rational surjection  $\pi'_f : j(Z) \rightarrow C$ . For any  $A \subset j(Z) \setminus j(C \times C)$  the image of  $\pi'_f(j(A))$  is a point. Hence any such  $A$  is contained the closure of the fiber of  $\pi'_f$  which is equal to  $j(Z_f)$ . On the other hand,  $j(C \times C)$  does not contain any abelian subvariety and hence the above statement holds for any abelian subvariety in  $j(Z)$  or equivalently in  $j(C^{(2)} \times C^{(2)})$ .  $\square$

**Corollary 10.19.** *If  $C$  is smooth plane curve of degree 5 then any abelian subvariety of  $j(Z)$  is contained in one of the  $j(Z_f)$ . Moreover, a maximal abelian subvariety  $A \subset j(Z) \subset j(C^{(2)} \times C^{(2)})$  is necessarily of dimension 2 and it exists only if there as an action of  $\mathbb{Z}/2$  on  $C$ . In this case  $g(C/\mathbb{Z}/2) = 2$  and  $A = J(C/\mathbb{Z}/2)$ . There is exactly one such subvariety for any subgroup  $\mathbb{Z}/2$  in the group of automorphisms of  $C$ .*

*Proof.* The number of ramification points is at most 6 since they are contained in a union of a  $\mathbb{Z}/2$ -invariant point and a line in  $\mathbb{P}^2$ . By the genus calculation,  $g(C/\mathbb{Z}/2) = 2$ . This curve defines an abelian surface in  $J$ .  $\square$

This completes the proof of the main theorem apart from the case of a trigonal curve  $C$ .

**Lemma 10.20.** Let  $C$  be a smooth projective curve of genus  $g(C) > 4$ . If  $C$  has a trigonal structure then it is unique.



*Proof.* Two distinct structure would give a rational embedding of bidegree  $(3, 3)$  into  $\mathbb{P}^1 \times \mathbb{P}^1$ . The genus computation shows  $2g_a(C) - 2 = (3, 3) \cdot (1, 1) = 6$ , where  $g_a(C)$  is the arithmetic genus of the image of  $C$ . Hence  $g_a(C) = 4$  and  $g(C) \leq g_a(C)$ , contradiction.  $\square$

**Lemma 10.21.** Assume that  $C$  is trigonal curve of genus  $g > 4$ , with a projection  $h : C \rightarrow \mathbb{P}^1$  of degree 3. Then  $j(C^{(2)} \times C^{(2)}) \subset J$  contains no abelian subvarieties.

*Proof.* First of all,  $C$  is neither bielliptic, nor hyperelliptic, nor a plane curve of degree 5 (cf. [AH91]). Moreover, the trigonal structure is unique (see [ACGH85]). Each point  $c \in C$  defines a degenerated 4-gonal structure. Apart from these, there are only finitely many other 4-gonal structures. Since the trigonal structure on  $C$  is unique there is no  $\mathbb{Z}/2$ -action on  $C$ , by the same genus estimate as in Lemma 10.14. Hence for any additional 4-gonal structure on  $C$  the curve  $C_f$  is irreducible.

We have two maps

$$\begin{aligned} \pi_c : C &\rightarrow C^{(2)} \\ c' &\mapsto c' + c \end{aligned}$$

where  $c \in C(k)$  and

$$\begin{aligned} \chi : C &\rightarrow C^{(2)} \\ c' &\mapsto c'' + c''', \end{aligned}$$

where  $c', c'', c'''$  are in the same fiber of the projection defining the trigonal structure.

It follows that

$$Z = \cup_f C_f \times C_f \bigcup_{c \in C(k)} (\pi_c(C) \cup \chi(C))^2 \subset C^{(2)} \times C^{(2)},$$

where  $f$  runs over a finite set of nontrivial 4-gonal structures.

Thus

$$j(Z) = \cup j(C \times C) \cup j(C^{(2)} \times \chi(C)) \bigcup \cup_f j(Z_f),$$

where  $f$  runs over (a finite set of) nondegenerate 4-gonal structures on  $C$ .

Note that  $j(C \times C)$  and  $j(Z_f)$  do not contain abelian subvarieties. Consider  $(x, y) \times (c, c'), (z, w) \times (s, s') \in C^{(2)} \times \chi(C)$ . Then

$$j((x, y), (c, c')) = j((z, w), (s, s'))$$

if

$$(x + y) - (c + c') = (z + w) - (s + s')$$

which is equivalent to  $x + y + c' = z + w + s'$ . The uniqueness of the trigonal structure implies that  $(x, y) = (c, c')$  and  $(z, w) = (s, s')$ . Hence the additional gluing in  $j(C^2 \times \chi(C))$  occurs only on the diagonal in  $\chi(C) \times \chi(C)$ .

Thus there are no abelian subvarieties in  $j(C^{(2)} \times C^{(2)})$ .  $\square$

## References

- [Abr94] D. ABRAMOVICH – “Subvarieties of semiabelian varieties”, *Compositio Math.* **90** (1994), no. 1, p. 37–52.
- [ACGH85] E. ARBARELLO, M. CORNALBA, P. A. GRIFFITHS and J. HARRIS – *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften, vol. 267, Springer-Verlag, New York, 1985.
- [AH91] D. ABRAMOVICH and J. HARRIS – “Abelian varieties and curves in  $W_d(C)$ ”, *Compositio Math.* **78** (1991), no. 2, p. 227–238.
- [BF66] R. BRAUER and W. FEIT – “An analogue of Jordan’s theorem in characteristic  $p$ ”, *Ann. of Math. (2)* **84** (1966), p. 119–131.
- [Box92] J. BOXALL – “Autour d’un problème de Coleman”, *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), no. 10, p. 1063–1066.
- [BT04] F. BOGOMOLOV and Y. TSCHINKEL – “Reconstruction of function fields”, 2004, [arXiv:math.AG/0303075](https://arxiv.org/abs/math/0303075), to appear in GAFA.
- [BT05a] F. BOGOMOLOV and Y. TSCHINKEL – “Curves in abelian varieties over finite fields”, *Int. Math. Res. Not.* (2005), no. 4, p. 233–238.
- [BT05b] —, “Rational curves and points on  $K3$  surfaces”, *Amer. J. Math.* **127** (2005), no. 4, p. 825–835.
- [CZ02] P. CORVAJA and U. ZANNIER – “Finiteness of integral values for the ratio of two linear recurrences”, *Invent. Math.* **149** (2002), no. 2, p. 431–451.
- [How96] E. W. HOWE – “Constructing distinct curves with isomorphic Jacobians”, *J. Number Theory* **56** (1996), no. 2, p. 381–390.
- [Hru96] E. HRUSHOVSKI – “The Mordell-Lang conjecture for function fields”, *J. Amer. Math. Soc.* **9** (1996), no. 3, p. 667–690.
- [IKO86] T. IBUKIYAMA, T. KATSURA and F. OORT – “Supersingular curves of genus two and class numbers”, *Compositio Math.* **57** (1986), no. 2, p. 127–152.
- [Kat02] N. M. KATZ – *Twisted  $L$ -functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002.
- [PS03] F. POP and M. SAÏDI – “On the specialization homomorphism of fundamental groups of curves in positive characteristic”, Galois groups and fundamental groups, Math. Sci. Res. Inst. Publ., vol. 41, Cambridge Univ. Press, Cambridge, 2003, p. 107–118.
- [Ray02] M. RAYNAUD – “Sur le groupe fondamental d’une courbe complète en caractéristique  $p > 0$ ”, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, p. 335–351.
- [Tam04] A. TAMAGAWA – “Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups”, *J. Algebraic Geom.* **13** (2004), no. 4, p. 675–724.
- [Tat66] J. TATE – “Endomorphisms of abelian varieties over finite fields”, *Invent. Math.* **2** (1966), p. 134–144.
- [Wei84] B. WEISFEILER – “Post-classification version of Jordan’s theorem on finite linear groups”, *Proc. Nat. Acad. Sci. U.S.A.* **81** (1984), no. 16, Phys. Sci., p. 5278–5279.
- [Zar] Y. ZARHIN – “Homomorphisms of abelian varieties over finite fields”, 2008.